MODÜL 1
BİLGİ VE İLETİŞİM TEKNOLOJİSİ KAVRAMLARI 2

1.3 Hergün Bilişim

1.3.1 Elektronik Dünya

1.3.1.1 Bilişim Teknolojileri

Bilişim teknolojisi; bilginin üretimi, bilginin başka insanlara öğretilmesi, bilginin kullanımı, bilgiye erişim yöntemleri, bilginin saklanması gibi birbiriyle ilişkili pek çok unsurun bir araya gelerek oluşturduğu yenilikçi teknoloji olarak tanımlanmaktadır (Güneş, Bilişim Toplumu, 2006). Bu teknoloji bilginin toplanmasında, işlenmesinde, depolanmasında, ağlar aracılığıyla bir yerden bir yere iletilmesinde ve kullanıcıların hizmetine sunulmasında yararlanılan iletişim ve bilgisayar teknolojilerini de kapsamaktadır. Ya da bu süreçleri kapsayan bütün teknolojiler **bilişim teknolojisi** olarak adlandırılmaktadır.



Geçtiğimiz yüzyılın sonlarında meydana gelen birtakım teknolojik gelişmeler tarım toplumundan sanayi toplumuna geçişi gerçekleşmiştir. 20. yüzyılın ikinci yarısında ise teknolojideki hızlı gelişmeler ve ileri teknolojilerin insan hayatına çok yoğun bir şekilde girmesiyle birlikte sanayi toplumundan bilgi toplumuna geçiş gerçekleşmiştir (Akın, 2006). Bu geçişin temelinde bilgi ile teknolojinin bütünleşmesi temel etken olarak görev almıştır. Bu bütünleşmeyle bilgi teknolojisi bilgi toplumunun en belirleyici göstergelerinden birisi haline gelmiştir. Bilgi toplumu, insanların bilgi teknolojilerini kullanarak yeteneklerini ortaya koyabilmesi ve kendini ispatlayabilmesi için önemli fırsatlar sunmuştur. Bilgi toplumunda bilginin temel özellikleri, sürekli üretilebilmesi ve artış gösterebilmesi, iletişim ağları içinde taşınabilir, bölünebilir ve paylaşılabilir olmasıdır. Bilginin temel özelliklerinin bu şekildeki değişimi bilgi teknolojilerinin gelişiminin bir sonucudur (Şeker, 2006).

Bilgi toplumuna geçişle birlikte günümüzde bilginin önemi giderek artmış, buna bağlı birçok yeni sektör ortaya çıkmıştır. Bu sektörlerden biri olan bilgi sektörü çağımıza damgasını vurmuştur. Gelişmiş ekonomilerde bilgi sektörü diğer bütün sektörleri geride bırakarak en büyük sektör haline gelmiştir. Bu değişimi vurgulayan **bilgiye dayalı ekonomi** (information-based economy) terimi bu gelişimin doğurduğu bir kavram olarak karşımıza çıkmaktadır (Tonta, 2006). Bilgiyi toplamak, işlemek, düzenlemek, depolamak, bir yerden bir yere aktarmak ve bu bilgiye erişmek için kullanılan bilgi teknolojisi ekonomik yapıda ciddi bir dönüşüm yaratmıştır (Acun, Bilişim, Bilgi Teknolojisi ve Türkiye, 1998).

1.4.1.2 Müşteriler için İnternet Servisleri

e-Ticaret (e-Commerce): Gelişen ve değişen dünyamızda teknolojik yenilikler ve bu yeniliklerin iş yapma şekilleri üzerindeki etkisi sürekli bir biçimde hayatımızın hemen tüm alanlarına girmekte ve değiştirmektedir. Bu değişimlerin sonucu olarak daha fazla rekabet, daha iyi ve hızlı hizmet, daha düşük maliyet, daha güvenli işlemler ve rahatlık açılarından uygun çözümler üretme ihtiyacı ortaya çıkmaktadır. Üretilen çözümlerden biri olarak ortaya çıkan elektronik ticaret hayatımızı, iş yaşamımızı ve ticari faaliyetlerimizi kolaylaştırmakta, hızlandırmakta ve daha rahat hale getirmektedir. Elektronik ticaret, tüm dünyada ticaretin

serbestleştirilmesi eğilimi ile birlikte, son on yılda yaşanan ve bilgi iletişimini kolaylaştıran teknolojik gelişmelerin bir ürünü olarak ortaya çıkmıştır. İnternet'in hızla yaygınlaşması, elektronik ticareti, ticari işlemlerin yürütülmesinde yeni ve çok etkin bir araç haline getirmiştir (Bulut, Öngören, & Engin, 2006).



Elektronik ticaret, mal ve hizmetlerin üretim, tanıtım, satış, sigorta, dağıtım ve ödeme işlemlerinin bilgisayar ağları üzerinden yapılmasıdır. E-Ticaret, her türlü malın ve servisin bilgisayar teknolojisi, elektronik iletişim kanalları ve ilgili teknolojiler (akıllı kart-smart card-, elektronik fon transferi -EFT-, POS terminalleri, faks gibi) kullanarak satılması ve satın alınmasını kapsayan bir kavramdır. Bu kavram işletme ile işletme ya da işletme ile son kullanıcı arasında yapılan ticari faaliyetleri kapsamaktadır (Akın H. B., 2000 Yılına Doğru Bilgi Toplumu Üzerine Genel Bir Değerlendirme ve Bilgi Ekonomisinin Özellikleri, 2006).

Elektronik ticaret; kamu kurum ve kuruluşları, bireyler, kurumlar ve firmaların da dahil olduğu dört türde gerçekleştirilmektedir (Güleş, Bülbül, & Çelebi, Küçük ve Orta Ölçekli Sanayi İşletmelerinde Elektronik Ticaret Uygulamaları, 2006):

Firma-Firma (B2B): Firmaların elektronik ortamda tedarikçiye sipariş vermesi, faturalarını temin etmesi ve bedellerini ödemesi bu bölümde değerlendirilmektedir. 1999 yılı verilerine göre; Firma-Firma kategorisindeki ticari işlemler, E-Ticaret cirosunun %90'nını oluşturmaktadır.

Firma-Müşteri (B2C): WWW teknolojisindeki hızlı gelişmeler sonucunda ortaya çıkan sanal mağaza uygulamaları ile İnternet'te firmaların elektronik ortamda; bilgisayardan otomobile, kitaptan pizzaya birçok ürünün doğrudan tüketiciye satışının yapmasıyla gelişen elektronik ticaret kavramıdır.

Firma-Kamu (B2G): Firmalar ile kamu kuruluşları arasındaki ticari işlemleri kapsayan bu bölümde kamu ihalelerinin İnternet'te yayınlanması ve firmaların elektronik ortamda teklif vermeleri ilk örnekleri oluşturmaktadır. E-Ticaretin yaygınlaşmasını desteklemek amacı ile kamunun vergi ödemeleri, gümrük işlemleri de sanal dünyaya taşınmaktadır.

Birey-Kamu (G2C): Henüz örnekleri çok yaygın olmasa da bu kategoride ehliyet, pasaport başvuruları, sosyal güvenlik primleri ile vergi ödemeleri, vb. uygulamalar ile e-devlete geçiş amaçlanmaktadır.



e_bankacılık: Bilişim teknolojilerinin yardımıyla en hızlı gelişen ve hizmet sunumunu çeşitlendiren sektörlerden biri bankacılık ve finans sektörüdür. İnternet'in getirdiği olanakları da bu gelişme doğrultusunda etkili bir araç olarak kullanan bankalar, e-bankacılık hizmetlerinde servis alanını yaygınlaştırmakta hem de müşterilerini e-bankacılığı kullanma konusunda teşvik etmektedirler. e-bankacılık, İnternet üzerinden bankanızla bağlantı kurarak hesaplarınıza ulaşabilmeniz, sorgulama yapabilmeniz ve

bankanızın sağladığı çeşitli işlemleri gerçekleştirmeniz anlamına gelmektedir. 1998'lerden sonra, İnternet bankacılığının ortaya çıkmasıyla birlikte şube bağımlılığı kısmen ortadan kalkmıştır.

Güvenlik açısından oldukça etkili bir sistem olan SSL güvenlik ve şifreleme protokolünün uygulanmasıyla birlikte e-bankacılık, güvenlik altyapısı anlamında şube bankacılığı kadar etkili bir yapıya kavuşmuştur. SSL güvenlik sistemleri kullanan Web sunucularında servis veren bankalar, müşterilerine kendi hesaplarına Web tarayıcısı kullanarak erişme imkânı sunmaya başlamışlardır. SSL sayesinde banka müşterileri (kendilerine ait müşteri numarası ve şifresini kullanarak) bireysel hesaplarına (interaktif hesap) güvenli bir şekilde erişerek, kendisi ile banka arasında kurulan güvenli Web oturumunda, para çekme dışındaki bütün bankacılık hizmetlerini kendi başına yapabilmektedirler.

Şube bankacılığının aksine e-bankacılıkta, zaman ve mekândan bağımsız yılın 365 günü ve 24 saat kesintisiz hizmet verebilmesi işlem yapabilme avantajı büyük kolaylıklar sağlamaktadır. Günümüzde e-bankacılığı kavramının içinde yer alan hizmetler oldukça artmıştır. Hesap bakiyesini öğrenmek, hesaplar arasında EFT/havale yapmak, virman yapmak, repo, yatırım fonu alıp satmak, hazine bonosu alıp satmak, kredi kartı işlemleri yapmak, fatura borcu ödemeleri yapmak, hisse senedi alım satımı yapmak, otomatik ödeme talimatları vermek, döviz alım satımı yapmak, fon alım satımı yapmak gibi hizmetler bunlardan birkaçıdır. e-bankacılığın, bankacılık faaliyet giderlerini düşüren bir uygulama olması, müşterilerini buna yöneltmeye teşvik edici ana unsurlardan biridir.



e-devlet: Kamu hizmetlerinde etkinliğin ve verimliliğin artırılması, katılımcılığın ve hesap verebilirliğin sağlanarak demokrasinin güçlendirilmesi, hizmet kalitesinin artırılması gibi nedenlerle birçok ülkede kabul gören elektronik devlet hizmetlerinin geniş ölçekli uygulamalarla geliştirilmesi gereği, ülkemizde de tüm kesimler tarafından kabul görmekte ve çok çeşitli uygulamalar hizmete konmaktadır. Kamu kurum ve kuruluşları, birçok alanda elektronik veritabanı ve otomasyon projeleri geliştirmişler ve İnternet üzerinden çeşitli uygulamaları hayata geçirmişlerdir. Ülkemizde de verilen çeşitli e-hizmetler giderek artmaktadır. https://www.turkiye.gov.tr/ adresinden ulaşabileceğimiz e-hizmetlerden birkaçı şunlardır: Motorlu Taşıtlar Vergi Borcu'nun Plaka No, Vergi Kimlik No ve Tescil Tarihi ile sorgulanması. Ödenen SSK prim dökümünün sorgulanması. SSK'dan ne zaman emekli olunabileceğinin hesaplatılması vb. tesisat ve daire numarası ile belediyelere olan borçların sorgulanabilmesi. Kurumlar Vergi Dairesi ile ilgili işlemlerin yapılabilmesi. Telefon faturası borcunun öğrenilip ödenebilmesi. Aşağıda ülkemizde de çok çeşitli uygulamaları bulunan belirli e-devlet hizmetleri kısaca açıklanmıştır.

Nüfus Bilgileri Kayıt Sistemi: Nüfus kayıtlarına çevrim-içi ortamda doğrudan ve hızlı erişim sağlamak amacıyla geliştirilen sistemlerdir. Bu sistemleri kullanan devletler genellikle vatandaşlarına birer kimlik numarası vererek, nüfus kayıtlarını bilgisayar ortamına aktararak, merkezi nüfus veri tabanını kurulmasını sağlamaktadırlar. Bu sayede bu verilerin farklı kurumlarda tekrar edilmesinin ve dolayısıyla kaynak israfının önüne geçilmesi, bu verilere erişim için harcanan mesai ve teknik araç gereçten de tasarruf edilmesi amaçlanmaktadır.

Trafik Bilgi Sistemleri: Karayolu trafiği ile ilgili bilgilerin (sürücü, araç, yol, kaza, ceza, ehliyet vb.) kayıt ve analiz edildiği, daha etkili tedbirlerin alınmasına ve karayolu trafik güvenliğinin geliştirilmesine yarayan sistemlere trafik bilgi sistemleri adı verilmektedir. Trafik bilgi sistemleri karayolu trafik güvenliği problemlerini objektif olarak değerlendirmek için gerekli olan e-devlet uygulamalardan biridir.

Vergi Kayıt Sistemleri: Vergi dairesi işlemlerinin tümünün bilgisayarlarla yapılarak iş yükünün azaltılması, vergi dairesi çalışmalarında etkinlik ve verimliliğin artırılması ve bilgisayar ortamında toplanan bilgilerden sağlıklı bir karar destek ve yönetim bilgi sisteminin oluşturulmasının hedeflendiği sistemlerdir.

Hastane Bilgi Yönetim Sistemleri: Sağlık kurumlarının bütün kaynaklarının (zaman, insan gücü, mal, finans) etkin bir şekilde kullanılmasına olanak sağlayan tümleşik sistemlerdir. Bu kurumların gelir/giderlerinin hatasız izlenerek kaçaklarının önlenmesi, kaynaklarının verimli olarak kullanılması, verilerinin hızlı/güvenli bir ortamda değerlendirilerek çağdaş bir yapıya kavuşturulması ve tüm birimler arasında uyumlu çalışma ortamının sağlanması amacıyla kullanılmaktadır.

Sağlık Bilgi Sistemi / E-Sağlık: Amacı erişim hakları tanımlanmış yetkili kişi ve kuruluşlarca ulaşılabilir, tüm vatandaşları kapsayan, her bireyin kendi bilgilerine erişebildiği, doğum ile başlayıp tüm yaşam süresince sağlıkla ilgili verilerinden oluşan işlevsel bir veritabanının; yüksek bant genişlikli ve tüm ülkeyi kapsayan bir iletişim omurgasında paylaşılmasıdır. Bu sistemler ülke genelinde sağlık hizmeti sunumu, finansmanı ve tedarikinde yer alan tüm kamu kurumları ile özel sektör kuruluşlarını kapsayan e-devlet uygulamalarıdır.

Hasta Takip Sistemi (HTS): Bu sistem ile devletler sağlık hizmeti alan vatandaşlarına ait kişisel sağlık kayıtlarının oluşturulması sağlanmaktadır. Bu sayede ulusal düzeyde kişisel sağlık kayıt içeriğinin belirlenmesi ve Aile Hekimliği Sistemi gibi sağlık uygulanmalarının gerçekleşmesi sağlanmaktadır.

Eczane Otomasyon Sistemi: Eczane Otomasyonu Sistemi özellikle reçete girişi ve takibi işlemlerini kolaylaştırmak amacıyla geliştirilmiş bir e-devlet uygulamasıdır. Uygulama ile gerek İnternet gerekse Sağlık Bakanlığı uzaktan erişim hatları üzerinden işlemlerin otomatik olarak yapılabilmesi sağlanmaktadır. Yalnızca anlaşmalı eczanelerin kullanabildiği bir yazılım ile 7/24 çalışan bu sistemle, emekli, çalışan, sigortalı, ilaç ve hastane sorgulamaları yapılabildiği gibi reçete girişi, faturalama işlemleri de gerçekleştirilebilmektedir.

1.4.1.3 e-Öğrenme

Bilgisayarların eğitime oldukça yararlı katkıları bulunmaktadır. Her düzeyde okul eğitime yardımcı olarak bilgisayar kullanmakta ve buna paralel olarak da yeni araç ve yöntemler geliştirilmektedir. Bilgisayarlı öğrenci kayıt sistemleri, okul ve dershaneler için zamanlama ve çizelgeleme sistemleri, bilgisayar destekli eğitim uygulamaları, uzaktan eğitim uygulamaları İnternet üzerinden ev ödevi uygulamaları gibi çalışmalar bu gelişimin sonuçlarından birkaçıdır.

Eğitim kurumlarında kullanılan e-öğrenme sistemleri sayesinde öğrencilerin, öğretim elemanlarının ve diğer eğitim kurumu çalışanlarının bu iş süreçleriyle ilgili işlemlerin otomasyonu amaçlamaktadır. Bu sistemlerle öğrencilere sunulan her türlü hizmetin mümkün olabildiğince zamanında ve etkin bir biçimde bilgi ve iletişim teknolojileri aracılığı ile

sunulması sağlanmaktadır. Genellikle bu sistemlerle öğrencilerin İnternet bağlantısı sağlayabilecekleri herhangi bir noktadan ders programlarını görebilmeleri, kayıtlarını yapabilmeleri, diğer akademik ve kişisel bilgilerine ulaşabilmeleri ve gerektiğinde verilen yetki çerçevesinde güncelleştirebilmeleri sağlanmaktadır.



Bu sistemlerle dönem içerisinde, hangi dersin ne zaman hangi içerikte işleneceğini İnternet'ten öğrenebilmekte, ilgili ders içeriğinin yer aldığı Web sayfası üzerinde; yazılı, işitsel ve görsel malzeme, video kayıtları, pdf, html biçiminde dokümanlar bulabilmekte ve bağlantılarla orijinal sayfalara yönlendirilebilmektedir. Burada bulunan yayınlara, çeşitli konulardaki yazılara ve makalelere ulaşabilmekte, arşiv taraması yapabilmektedirler. Aynı şekilde öğretim elemanları, bölüm sekreterleri ve diğer eğitim kurumu personelinin de ihtiyaç duydukları işlemlerin çevrim-içi olarak yapılabilmesine olanak sağlayan daha kapsamlı sistemler de e-öğretim içerisinde kullanılmaktadır.

e-Öğrenme Özellikleri: Bilgi toplumu ve hızla gelişen yeni ekonomi eğitim alanında da etkisini göstermiş ve köklü değişiklere neden olmuştur. Bilgiye ulaşmada zaman ve mekân açısından büyük yararlar sağlayan İnternet; eğitim materyallerinin (kitap, çalışma notları, makale ve bilimsel yayınlar vs.) hızla artması, öğrenci ve öğretmenlerin bu malzemelere kolayca ulaşabilmesi ve dolayısı ile kendilerini geliştirebilmelerinde anahtar rol üstlenmektedir. Bu yaygınlık İnternet üzerinden e-öğrenme uygulamaları gibi çalışmaların yapılabilmesine olanak vermektedir.



Günümüzde gittikçe yaygınlaşan ve çoğu üniversitenin de hızla altyapı hazırlıklarını tamamladığı e-öğrenmenin birçok olumlu özelliği bulunmaktadır. Bunlardan bazıları şunlardır:

- Öğrenci merkezlidir.
- Öğrenci konuyu öğrenene kadar, konu üzerinde çalışabilir. Herkes kendi öğrenme hızında öğrenebilir.
- Zaman sınırsızdır. Esnek öğrenme zaman sunar
- Öğrenci, konuyu anlamadığı zaman, iletişim araçları ile öğretmen ve diğer öğrenciler ile bağlantı kurabilir.
- Dünyanın diğer ucundaki bir kişinin bilgilerinden faydalanılabilir.
- Bağlantılar aracılığıyla, doğru ve istenilen kaynağa kısa sürede erişilir.
- Eğitim maliyetlerini dikkate değer anlamda düşürmektedir.
- Zaman ve mekândan bağımsızdır. 7/24 açık öğrenme ortamı sunar. Kişi kendini en rahat hissettiği zaman ve mekânda konuyu öğrenebilir.
- Öğrenim faaliyeti daha zevkli olabilir. Çoklu ortam öğrenme tecrübeleri sunar.
- Öğrenim materyalleri, hızlı değişen koşullara göre, kısa sürede güncellenebilir.
- Kişisel testler ile öğrenci kendi kendini sınayabilir.
- Konunun anlaşılıp anlaşılmadığına dair geri bildirimin hızlı bir şekilde yapılması motivasyonu artırır.

- Kişinin tüm öğrenim faaliyetleri raporlanabilir.
- Her tür altyapıdan ve toplumun farklı kesimlerinden gelen öğrencilere fırsat eşitliği sunar.

1.4.1.4 Tele Çalışma (Teleworking)



Çevrim-içi organizasyonların gelişimiyle beraber çalışma şekillerinde ve mekânlarında da büyük değişiklikler meydana gelmiş, iş mekânları tartışılmaya başlanmış, niçin iş için bir mekânın zorunlu olması gerektiği sorgulanmaya başlanmıştır. Bu tartışmaların sonucu olarak ortaya çıkan Tele Çalışma yani uzaktan çalışma ya da evde çalışma olarak adlandırılan standart dışı çalışma biçimleri giderek ağırlıklı biçimde görülmeye başlanmıştır. Uzaktan çalışma, bilgi teknolojilerinin ve telekomünikasyonun hızlı gelişimiyle beraber ortaya çıkan bir kavramdır. Bu teknolojilerin sağladığı avantajlarla insanlar dokümanlar içinde aynı binada çalışma ihtiyacından kurtulmuşlardır. Uzaktan çalışma, işlerini yapmak için ofise gitmeye ihtiyaç duymayan çalışanlar için kullanılan bir kavram haline gelmiştir.

Uzaktan çalışan kişiler bağlı oldukları kurum ya da diğer çalışanlar ile iletişim kurmak için İnternet'e bağlı bir bilgisayar, modem, tarayıcı, bilgisayar yazılımı, yazıcı, onlara tahsis edilmiş bir telefon hattı, faks cihazı vb. kullanılmaktadır. Bunların ve özel ofis mobilyalarının bulunduğu ayrılmış bir mekân bir çalışan evinde, otelde ya da herhangi bir yerde olabilir. Aslında yapılan çalışma biçimine göre gerekler değişmektedir. Örneğin yanlarında taşınabilir bilgisayar ya da akıllı telefonlarıyla arabalarında, yolda, müşterilerinin yanında, bir başka şehirde ya da bir başka ülkede, her yerde uzaktan çalışmak mümkün olabilmektedir.

Sanal işyerinde, iş zamandan ve ortamdan bağımsızdır ve süreçler üzerinde odaklanmıştır. Süreçler, süreklilik halindedir. İşin çok belirli bir başlangıç ve bitiş noktası yoktur. İş, yapı ve sanal ürünün dinamikleriyle yürür. Sanal işyeri görsel ve fiziksel yakınlıklarla sınırlanmamıştır. Bu nedenlerle gerek işveren gerekse çalışan için birçok avantaj sağlamaktadır. Uzaktan çalışmanın sağladığı temel avantajlar şunlardır (Aslan, 2006):

- %30 ofis ve yer giderlerinden kesinti sağlar. Ofis malzemeleri ve mobilya maliyetlerini düşürür.
- %40 ya da daha fazla performans artışı sağlar. Çalışma saatlerinde büyük esneklik sağlanır.
- Uzaktan çalışma, seyahat zamanını ortadan kaldırır.
- Organizasyonun esneklik ve hareket kabiliyetini arttırır ve kazanma becerisinin takımlara adapte edilmesini sağlar. Verimliliği artırır.
- Uzaklık kavramı yok olmaktadır. Organizasyonlar böylece çok uzakta dahi yaşasalar da onlar için gerekli olan çalışanı çalıştırma olanağına sahip olurlar.
- Çalışırken rahatsız edilme duygusunu ortadan kaldırır.
- Çalışanların sürat ve de sorumluluk duygusunda artış olur.

Uzakta çalışmanın avantajlarının yanında bazı dezavantajlarının da bulunduğu görülmektedir. Bu durum daha çok uygulamanın kendisinden kaynaklanan bir sonuçtur. Görülen dezavantajlar şunlardır (Aslan, 2006):

- En büyük dezavantajı sosyal faktörlerdir. Takım ruhunun olmayışı. Çalışanların organizasyon kültürüne uzak ve de yabancı kalabilmesi. Uzaktan çalışan bireylerde bir yalıtma sorunu ve kendilerini bir organizasyon ait hissedememe durumu ortaya çıkabilmektedir.
- Çalışanların ofisteki araçlardan ve de diğer avantajlardan yararlanamamaları.
- Çalışanların sosyal etkileşimden ve değişik fikirleri paylaşmaktan uzak kalmaları en çok görülen dezavantajlardır.

1.4.2 İletişim

1.4.2.1 Elektronik Posta



Elektronik posta ya da kısa adıyla e-posta, İnternet üzerinde bilgisayarlar ve insanlar arasında yazılı bilgi alışverişini sağlayan ve en yaygın kullanılan İnternet uygulamasıdır. Bilgisayar ağlarının oluşturulma nedenlerinden biri de, kişilerin, bir yerden diğerine (hızlı ve güvenli bir şekilde) elektronik ortamda haberleşme isteğidir. Bu isteği hızlı ve güvenli bir şekilde e-posta sağlamaktadır. E-posta, günümüzde en ucuz ve hızlı haberleşme araçlarından birisi olmuştur.

Bir e-posta adresine sahip herkes, e-posta adresini bildiği birine hızlı bir şekilde bir mektup gönderebilir. Burada şart bu mektubun gideceği bir geçerli adresin olma zorunluluğudur. Elektronik ortamda bu adrese, **e-posta adresi** denir. E-posta adresi **@** işareti ile ayrılmış iki kısımdan oluşmaktadır. İlk kısım kişinin kendi isminden ya da seçtiği bir takma isimden oluşur. İkinci kısım ise, e-posta adresini aldığı sunucu sistemin adresini belirtir. Örneğin aliyasar@gmail.com veya musti@e-kolay.net gibi. Günlük hayatta kullanılan postaya benzer şekilde, her e-postanın bir göndereni vardır; ancak klasik postadan farklı olarak birden fazla alıcısı olabilmektedir.

E-posta istemci/sunucu prensibi ile çalışan bir uygulamadır. Posta okumak ve göndermek için kullanıcılar postaların geldiği ve gönderildiği bilgisayara, yani sunucuya erişmek zorundadırlar. İnternet Servis Sağlayıcıların (ISS) sunucu bilgisayarlarında posta kutusu görevi yapan bir e-posta sunucu yazılımı bulunur. Yani size gelen mesajlar bu posta kutularında birikirler. Bunların alımı amacıyla kullanılan istemci yazılım, kullanıcının postayı okumasını, postaya cevap göndermesini, postayı yönlendirmesini veya yeni posta yazmasını ve bunu göndermesini sağlayan programdır. Kullanılan E-posta programında ISS'nın belirttiği ayarları yaptıktan sonra Al komutu vererek bu posta kutuları kontrol edilir ve size gelen mesajlar kullanılan sistemde okunabilir. Aynı şekilde e-posta programında yeni bir mesaj sayfası açılarak, karşı tarafın e-posta adresi belirtilerek bu adrese gönderilebilir. Bu aşamada yazılan e-posta adresinden hangi sunucuya gideceği belirlenir ve e-posta karşı tarafın posta kutusuna gönderilir. E-postalar genelde birkaç saniye içinde posta kutularına ulaşırlar, kullanıcıların tek yapması gereken, İnternet'e bağlanıp posta kutularını kontrol etmektir.

İnternet üzerinde TCP/IP protokollerinin bir parçası olan SMTP (Simple Mail Transfer Protocol) protokolüne dayalı e-posta sistemleri kullanılmaktadır. SMTP, e-posta mesajlarının İnternet’te rahat hareket etmelerini sağlayan bir protokol ya da kural kümesidir. Yaygın e-posta sistemlerinde SMTP’nin yanında POP (Post Office Protocol) adında ikinci bir servis hizmeti daha bulunmaktadır.

Evden, işyerinden yapılan bağlantılarda gelen e-postaları almak ve okumak için POP3'ü destekleyen e-posta programlarının (Eudora, Microsoft Outlook, vb.) kullanılmasıyla büyük avantajlar sağlar. Bu şekildeki kullanımda; kullanıcı posta sunucusuna kendi bağlanmadan sunucusunda bulunan posta kutusundaki tüm e-postaları kısa sürede kullandığı bilgisayardaki posta kutusuna alınır; daha sonra bağlantı otomatik olarak kapatılır ve e-postalar okunabilir. İstenirse yazılan cevaplar, daha sonra tekrar bağlanarak SMTP servisi üzerinden gönderilebilir. Bu kullanım şekli kullanıcısına çok büyük zaman kazandırmaktadır.

E-postalarda kullanılan kısaltmalar ve anlamları aşağıda belirtilmiştir:

***From (Kimden)**:* E-posta'yı gönderen kişinin e-posta adresi (ve gerekli olmasa bile, Adı, Soyadı) yer alır.

***To (Kime)**:* E-posta'yı göndereceğimiz kişilerin e-posta adresleri yer alır. Birden çok kişiye gönderilecekse adresler aralara virgül konarak ya da bir boşluk bırakılarak yazılır.

***Subject (Konu)**:* E-posta içeriği kısa bir şekilde yazılır. (Merhaba, Önemli, Duyuru vb. gibi)

***Cc (Carbon Copy)(Bilgi)**:* E-postanın kopyasını başka bir kişiye ya da kişilere (genellikle, e-posta içeriği ile 2. dereceden ilgili kişiler olabilir) gönderilecekse, onların adresleri bu alana yazılır.

***Bcc (Blind Carbon Copy)(Gizli)**:* Cc ile aynı işlevi görür. Fakat e-postayı alan kişiler bu postanın gönderildiği diğer kişi ya da kişileri göremezler.

***Attachment (Eklenmiş Dosya)**:* E-postalarla birlikte, eğer istenirse, postanın sonuna eklenerek herhangi bir dosya da gönderilebilir. Buna Attachment (eklenmiş dosya) adı verilmektedir. Eklenen dosya, düz bir yazının yanı sıra resim, ses, program vb. içeren dosyalar da olabilir.

***Kullanılan Çeşitli Semboller ve Anlamları**:* Yazılarda kızgınlık, sevinç, üzüntü, şaşkınlık, merak vb. gibi duyguları ifade etmek için çeşitli işaretler kullanılmaktadır. Aşağıdaki kısaltmalar İnternet ortamında çok fazla kullanılan işaretlerdir. Bu işaretler klavyede yer alan iki nokta, tire ve parantez açma tuşları kullanarak kolayca elde edilebilir.

***:-)** veya **:)** Gülümsemek*
***:-)))))** Sırıtarak gülmek*
***:-(** veya **:(** Üzüntülü olmak*
***:'-(** Ağlamak*
***:-(((((** Çok üzülmek*
***:-o** Şaşırmak*
***;-)** Göz kırpmak*
***:-D** Kahkahayla gülmek*

1.4.2.2 Anlık Mesajlaşma



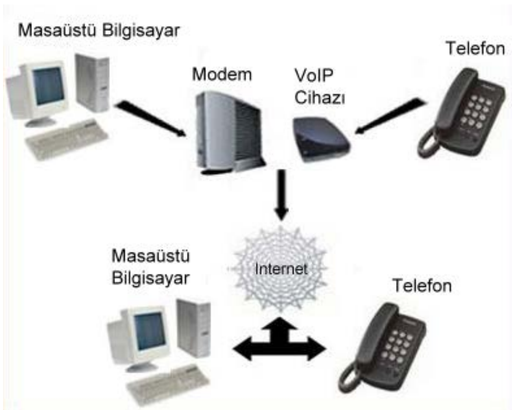
Anlık mesajlaşma, bir bilgisayar programı sayesinde, üye olarak, listenize eklediğiniz kişilerle gerçek zamanlı görüşme olanağıdır. Kullanıcının başka bir Internet kullanıcısına gerçek zamanlı mesaj göndermesinden oluşur. Program özelliğine bağlı olarak görüntülü ve sesli görüşme olanağı da olabilmektedir. En bilinen anında mesajlaşma programları Pidgin, Kopete, ICQ, Yahoo Messenger, MSN Messenger ve Google Talk'dır.

Anlık mesajlaşma kullanıcıların gerçek zamanlı olarak iletişim kurmalarını sağlayan bir uygulamadır. Kullanıcıların soru veya yorumlarına hızlı cevap verilebilir. Bu amaç için anında mesajlaşma mükemmel bir yöntemdir ve uzun mesafe telefon faturalarında ücretten tasarruf ederken aile bireyleri ve arkadaşlar ile temas halinde kalmasını sağlar.

Herhangi bir çevrimiçi etkinlikte olduğu gibi, anlık mesajlaşmada da çok dikkat edilmelidir. Sohbet odalarına davet edilen kişiler hakkında bilgi sahibi olmama durumunda çeşitli risklere girmek kaçınılmazdır. Ayrıca virüs, solucan ve truva atları mesajlaşma yoluyla sisteminize bulaşabilir ve bu nedenle güvenli olamadığı düşünülen kaynaklardan herhangi bir dosyayı kabul edilmemelidir.

1.4.2.3 VoIP

Voice Over IP (VOIP) teknolojisi, adından da anlaşılacağı üzere, herhangi bir IP Network'ü (Kiralık Hat, Frame Relay, ADSL, GSHDSL vs.) üzerinden ses veya faks iletişimi



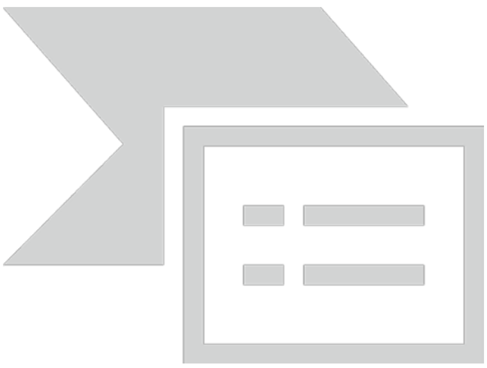
yapmak için geliştirilmiş bir teknolojidir. Bu sayede özellikle uzak noktalarla yapılan telefon ve faks iletişim maliyetleri çok ucuzlamakta ya da bedava olmaktadır. VOIP cihazlarının işgal ettiği bant genişliği 16Kbps gibi çok düşük değerlerden (Normal telefon hatları 64Kbps'dır) başladığı için, kullandıkları data hatlarında herhangi bir yavaşlamaya neden olmazlar. VOIP teknolojisi ile çalışan ürünler, mevcut IP ağı cihazları ve PBX santralinde herhangi bir değişiklik yapmadan, çok kısa süreler içinde var olan sisteme entegre edilebilir. VOIP cihazları özel bir santrale veya belli marka bir Router a bağımlı değildir. Temel özellikleri uygun olan her Router ve Santral ile çalışabilir. Bu da VOIP yatırımı maliyetini azaltan çok önemli bir faktördür. VoIP, 'V'oice 'o'ver 'I'nternet 'P'rotokol (İnternet protokolü üzerinden ses) açılımına karşılık gelmektedir. VoIP, ses'i (genellikle insan sesi) IP paketleri halinde bu protokolün kullanıldığı ağlar veya internet üzerinden taşımaktır.

Session Initiation Protokol (SIP), oturum başlatma protokolü olarak adlandırılır, bu protokol data hatları üzerinden multimedya oturumlarının başlatılması, yönetimi ve sonlandırılması gibi işlevleri gerçekleştirir. Her Voip cihazı içerisinde Sip hesap tanımlaması yapılır ve bir SIP Server'a oturum açılır.

Harici olan normal telefon hatlarını (PSTN, GSM vs.) arayabilmek için bir Voip hesabının olması gerekmektedir. Bu VoIP hesabı ile SIP Server'a oturum açılır ve görüşme sağlanabilir. Voip hesabı SIP Server barındıran Servis Sağlayıcılardan alınabilmektedir. Global Telekom http://www.globaliletisim.com.tr, Borusan Telekom http://www.bnet.net.tr ve Superonline http://www.superonline.com Vo-IP servis sağlayıcılarından bazılarıdır.

Voip hesabı ücretlidir ve Sip Server üzerinden arayacağınız harici hatlar içinde ücret tarifeleri mevcuttur. Bu ücretler normal telefon ücretlerine nazaran çok daha ekonomiktir. Voip ile sesli görüşme ücretsizdir ama eğer bir Servis Sağlayıcıdan Voip hesabı alınacak ise bu ücrete tabidir. Harici numaralara yapılan aramalarda ücretlendirilir. Fakat kendi Voip networkunuz arasında olan görüşmeler yine ücretsizdir ancak arada bir SIP Server olursa şube başına aylık 7-25 YTL arasında değişen sabit ücretler ödenmektedir. SIP Server hizmetini internet üzerinden ücretsiz (Free) olarak veren sağlayıcılarda vardır. http://www.freeworldialup.com buna örnek gösterilebilir.

1.4.2.4 RSS



RSS çeşitli internet siteleri tarafından yayınlanan haber vb. içeriğin tek bir ortamdan topluca izlenebilmesine olanak sağlayan yeni bir içerik besleme yöntemidir. **RSS** – **R**eal **S**imple **S**yndication, RDF Site Summary veya **R**ich **S**ite **S**ummary (Zengin Site Özeti) kelimelerinin baş harflerinden oluşan kısaltmadır. XML biçiminde olan RSS dosyaları ilk olarak NetScape firması tarafından geliştirilmeye başlanmıştır. RSS dosyalarının kullanımı her geçen gün artarak yaygınlaşmaktadır. Kullandığı dosya biçimleri .rss ve **.**xml'dir. RSS kısaltmasının açılımı ve zaman içinde gelişimi şöyledir:

- Rich Site Summary (RSS 0.91) (Zengin Site Özeti)
- RDF Site Summary (RSS 0.9 and 1.0) (RDF site Özeti)
- Really Simple Syndication (RSS 2.0.0) (Çok Basit Besleme)

RSS yöntemini destekleyen sitelerin hazırladıkları XML biçimli dosyalara birçok programla erişmek mümkündür. XML okuyucusu olan bu programlar, web gezgini veya e-posta istemcisi olabileceği gibi sadece RSS içeriği izlemek için hazırlanan masaüstü programları da olabilir. RSS ikonunu (RSS / / XML) gördüğünüz herhangi bir yerde, RSS verilerini RSS istemcisi kullanarak alınabilmektedir.

Genel olarak, RSS verilerini, XML dosyaları olduğu için Internet Explorer içinden görebilirsiniz. Ancak sayfayı devamlı yenilemek ve RSS verilerini bu şekilde izlemek çok da verimli bir yöntem değildir. Bunun için pek çok insan, bazı RSS istemcileri kullanarak RSS

verilerini takip eder. RSS veri "toplayıcıları", RSS verilerini toplamanız ve takip etmeniz için uygun arabirim sunarlar.

Multi-RSS feed reader, İnternet haber taşımacılığın neredeyse son noktasıdır. Çünkü birçok alt site, haber kaynağı olarak kullandığı siteleri kaynakça olarak göstermektedir. Ayrıca aldığı haberleri basit bir harmanlama yöntemi ile kendi sitesine haber yapar. "Multi-RSS feed reader" da ise bu işlemi otomatik bir şekilde PHP veya ASP desteği olan her site sahibi yapabilir. Türkçe ilk örneği http://www.tamiyi.com/'dur. RSS kullanmanın yararları şunlardır:

RSS sürekli internet başında zaman geçiren ve kullanan kişilere çok büyük kolaylık sağlamaktadır. Sürekli olarak beğendiğiniz sitelerin en son içeriklerini size getirerek en kolay şekilde bilgilenmenize olanak tanımaktadır. RSS ile her siteyi teker teker gezmeye gerek kalmamakta ve böylece zamandan tasarruf sağlanmaktadır. Her e-posta bültenine kayıt olmak zorunda kalınmadığı için, kullanıcıların kişiselliği ve gizliliği garanti altına almış olmaktadır.

1.4.2.5 Blog



Blog (ağ günlüğü, günce) veya Weblog (Ağ kütüğü) teknik bilgi gerektirmeden, kendi istedikleri şeyleri, kendi istedikleri şekilde yazan insanların oluşturabildikleri, günlüğe benzeyen web siteleridir. Blog, genellikle güncelden eskiye doğru sıralanmış yazı ve yorumların yayınlandığı, web tabanlı bir yayını belirtir. Çoğunlukla her gönderinin sonunda yazarın adı ve gönderi zamanı belirtilir. Yayıncının seçimine göre okuyucular yazılara yorum yapılabilir. Yorumlar, blog kültürünün çok önemli bir dinamiğidir; bu sayede yazar ve okuyucular arasında iletişim sağlanır. Bunun dışında, geri izleme mekanizmasıyla, belirli bir yazı hakkında yazılan diğer yazıların belirlenebilmesi de mümkündür.

İlk bloglar elle yazılıp güncellenirken, günümüzde bu amaçla özel yazılmış yazılımlar kullanılmaktadır. Bu yazılımlardan bazıları bir blog servisi sağlayıcı sitenin alt alan adları olarak yaratılabilen, bazıları ise kullanıcının kendi sunucusuna kurup çalıştırması gereken yazılımlardır.

Blogların içeriği geleneksel internet içeriğinden farklılık gösterdiği için sadece bloglar için kurulmuş özel indeksleme mekanizmaları ve arama motorları bulunmaktadır. Technorati en başarılı blog teknolojilerinden biridir. Ayrıca Google Blog Search adında bir blog arama motoru işletmektedir. Weblogs.com, dünyanın en büyük blog ping servisi olarak tüm internet indeksleme mekanizmalarına veri sağlamaktadır.

Belirli bir konusu olmayıp her hangi bir konu hakkında güncel haberler, olaylar, politika, günlük hayat, spor, teknoloji, müzik, yemek hatta bakkal Ali amcanın sorunları hakkında bile yazılar yazılabilen blogların çeşitli türleri bulunmaktadır. Bunlar:

Kişisel: İnternet üzerinde bireysel olarak oluşturulan, genel veya belli bir odak noktası olan blog çeşididir. Büyük oranda blog yazarının ismini veya takma adını alırlar. Yazarın bireysel günlüğü olmak dışında gündemi kendi kalemi ile yansıttığı ortamdır. Kişilerin günlük

yaşamda yaşadıkları olayları, karşılaştıkları durumları okurlarıyla paylaşmasını sağlar. Bloglarda en fazla rastlanan türdür.

Temasal: Sadece belirli bir alanda yazılan gönderilerin yer aldığı, belirli bir konuda uzman kişilerin yazdığı ve düzenlediği bloglardır. Politika, pazarlama, yemek, internet, ekonomi, tasarım, fotoğraf, programlama dilleri, blogger temaları ve benzeri konularda odaklanmış bloglar bulunmaktadır.

Topluluk: Üyelik sistemine sahip olan ve bu üyelerin yazdıkları gönderilerden meydana gelen bloglardır. Komünite olarak da adlandırılan bu türdeki blogların çoğu kendi sunucularındaki blog yazılımını kullanmaktadır.

Kurumsal: Şirketlerin kendileri ile ilgili haber ve duyurularını daha samimi bir şekilde halka açtıkları bloglar, dünyada ve iş hayatında giderek önem kazanmaktadır. Aslında bu alandaki akım, şirketin doğrudan değil, samimi karakterdeki bazı çalışanların desteklenmesi yoluyla bloglamaktır.

1.4.2.6 Podcast

Terim Apple'ın ürettiği taşınabilir müzikçalar iPod'un, adındaki **pod** ve İngilizcede "yayın" anlamına gelen "broadcast" sözcüğünün **cast** kısmı alınarak türetilmiştir. Podcast'ler ilk defa Apple iPod için geliştirilmiş olmasına rağmen günümüzde doğrudan iPod ile ilgili bir kavram değildir. Podcast kavramı Türkçemizde henüz bir karşılık bulmamasına rağmen "Oynatıcı Yayın Aboneliği" olarak kullanımı çok yanlış olmadığı varsayılmaktadır.



Yeni Oxford Amerikan Sözlüğü podcast'i 'Radyo yayını ya da benzer bir programın internetten çekilebilir ve kişisel ses cihazlarından dinlenebilir hale gelmesini sağlayan sayısal kayıt' olarak açıklamaktadır. Podcast sisteminin internetten bir programın ses ya da video kaydını çekmekten farkı RSS veya Atom beslemelerinin kullanılması ve böylece her yeni bölümü özel yazılımların izleyerek otomatik olarak yükleniyor olmasıdır.

Podcasting, çevrimiçi yayının üyelik gibi yollarla kullanıcılara ulaştırılmasıdır. Birçok podcast, MP3 ve görüntü dosyaları biçimlerinde olup RSS protokolüyle yayınlanır. Podcasting, kullanıcılarının herhangi bir zamanda kullanabildikleri dergi ya da belgesel gibi eğitici yönü olan yayınların hepsini içine almaktadır. Podcasting'in günümüzde özellikle eğitim amaçlı, tanıtım gibi alanlarda ve hatta emniyetten sorumlu kurumların dahi güvenlik amaçlı kullanımına girmiştir. Eğitim alanındaki işleviyle podcasting, öğrencilerin ve öğretmenlerin herhangi bir zaman ve yerde bilgiyi paylaşmalarını sağlayabilmektedir. Bu özelliğinden dolayı uzaktan eğitimdeki yeri oldukça önemlidir.

Podcast, bir oynatıcı için dağıtılan uygun ses ya da görüntü dosyası şeklindeki bir yayın dağıtım sistemidir. Kullanıcılar abonelik yöntemiyle bir dizi podcast’e ulaşabilir. Podcast’in kalbinde RSS (really simple syndication) özellikleriyle birlikte, XML (extensible markup language) dosyası yer almaktadır. Bu dosya ulaşılabilir olan tüm öğelerin ve bölümlerin listesini

barındırmaktadır. İçinde yer alan toplayıcı program, düzenli olarak kayıtlı dosyaları örneklenip yeni bölümleriyle otomatik olarak güncelleştirmektedir. Podcast'in gezici bir aygıtla dinlenebilmesi (PDA, akıllı cep telefonu, tablet pc, bilgisayar) onu etkin bir öğrenme aracı haline getirmektedir.

Podcast takip etmek isteyenler için bu konudaki en iyi program iTunes'dir. Juice, Podtower, Winamp, Zune, Amarok ise diğer alternatif podcast takip programlarıdır. Bu programlar ile birçok farklı konuda podcast bulabilir, hoşunuza gidenleri dinleyebilir, izleyebilir, abone olabilir ve bilgisayarınızda arşivleyebilirsiniz.

1.4.3 Sanal İletişimler

1.4.3.1 Sanal İletişimim İçeriği



Bilişim teknolojilerinin hızlı bir biçimde değiştiği, geliştiği günümüzde insanın olağan iletişim ihtiyacını gidermenin en kolay ve görece ucuz yollarından biri olarak sanal iletişim karşımıza çıkmaktadır.

"İletişim anlamların ortak hale getirilme sürecidir" şeklinde tanımlanırsa, bu sürecin gerçekleşme aşamalarında çeşitli bileşenler bulunmaktadır. Sanal iletişimde de, tıpkı iletişimin tanımında olduğu gibi bir kanal, alıcı (lar) ve verici (ler) bileşenleri söz konusudur. İletişimi sözlü (dilin kullanımı) ya da sözsüz (beden dilinin kullanımı) olmak üzere ikiye ayırabilirken, Sanal iletişimin sözcüklü simgeli görüntülü sesli çeşitleri söz konusudur. Sanal iletişimde "metin temelli araçlar", "sesli konferans araçları", "video konferans araçları" kullanılabilmektedir.

Metin temelli iletişim araçları; sohbet odaları, e-posta, tartışma listeleri, haber grupları, mesajlaşma sistemleri olarak sayılabilmektedir.

Sohbet odaları: 1988 yılında IRC (Internet Relay Chat) adlı protokolün geliştirilmesi ile ortaya çıkmış ve Körfez Savaşı'nda kullanılmıştır. Bu araç ile "kanal" a bir "takma isim" ile bağlanılır, meramımızı anlatabilmemiz anadilimizi "doğru, düzgün, yerinde kullanmamız- la" yakından ilgilidir.

e-posta: İletimizi (mesajımızı) birden çok kişiye aynı anda gönderebiliriz, iletimize belge ekleyebilir, gelen iletiler ve belgeler üzerinde çalışma (değişiklik/düzeltme) yapabiliriz.

Tartışma listeleri: Tartışma listeleri ile belli bir konuda birden çok kişi ile bilgi alış-verişinde bulunabilir; tanıdıklarınızla bağlantılarınızın (mezunlar listeleri vb.) devamlılığını sağlayabiliriz. Tartışma listeleri kontrollü veya kontrolsüz olabilmektedir. Kontrollü listelerde mesaj akışını kontrol altında tutması gereken bir kişinin (moderatör) varlığı şarttır. Kontrolsüz listelerde moderatör bulunmaz.

Haber grupları: Haber gruplarına katılabilmek için izin ya da davet almak gerekmektedir. Haber gruplarında iletiler çevrim içi okunmaktadır.

Mesajlaşma sistemleri: Mesajlaşma sistemlerinde metin dışında ses ve görüntü de iletilebilir. Birden fazla kişi ile de gerçekleştirilebilir. MSN Messenger, bu sistemlere örnek olarak artık hemen herkesin bildiği ve kullandığı bir sistemdir.

Sesli konferans araçları: Netmeeting, Skype ve İnternet telefonu ile bire bir, bire çok haberleşme olabileceği gibi çok kişinin çok kişi ile haberleşmesi de mümkündür.

Video konferans araçları: Netmeeting ve Skype. Ses dışında, görüntü iletmemizi de olanaklı kılan video konferans araçlarıdır. İletilecek veri, gönderen tarafta sıkıştırılmakta ve alıcı tarafta açılarak anlaşılır hale getirilmektedir.

Sanal Topluluk (Virtual Community): Sanal topluluklar, ortak bir ilgi alanını paylaşan ve İnternet üzerinden bilgisayarlar aracılığı ile bilgi ve görüş alış-verişinde bulunan insan topluluklarına verilen isimdir. Örnek olarak "bilgiguvenligi@yahoogroups.com" verilebilir. Bu topluluklarda bir grubun parçası olma duygusu. Parçası olunan grubun norm ve kurallarına uygun davranma durumu. Parçası olunan grubun rollerini üstlenme durumu gibi durum ve duygular söz konusudur.

Sosyal Ağ Siteleri: Buna kişilerin arkadaşlarıyla iletişim kurmak için kullandıkları araçlar/olanaklar sistemi denilebilir. Örneğin "Facebook" bir sosyal ağ sitesidir.

Bilgisayar Oyunları: İnternet kullanımı; bireyin araştırma yapması, kendi potansiyelini keşfetmesi ve zenginleştirmesi, sorun çözümü, hedefe ulaşmak için farklı yollar deneyimleme gibi tecrübeler edinmesine neden olması açısından zenginleştirici olabilmektedir.

1.4.3.2 İçeriği İnternette Yayınlama Yolları

Hazırlamış içeriklerin internette yayınlanabilmesi için çok çeşitli olanaklar bulunmaktadır. Bu olanaklar içeriğin türüne göre değişmekle birlikte hemen hemen her tür içeriğin (metin, fotoğraf, ses, video vb.) kişisel blog'larda, içerik yayını için hazırlanmış sitelerde (You Tube gibi) yayınlanabilmesi mümkündür.

Fotoğrafların yayınlanmasında çevrimiçi resim galerisi uygulamaları çok fazla sayıda fotoğrafın paylaşımı için etkili bir yöntemdir. Bu amaçla hazırlanmış birçok yazılım mevcuttur (öreğin JAlbum). Bu tür yazılımlarla hazırlanan albümün doğrudan çevrimiçi bir sunucuya



aktarılması sağlanmaktadır. Fotoğrafları çevrimiçi paylaşmak için yine çok sayıda ücretli ve ücretsiz uygulama bulunmaktadır. Eğer çok sayıdaki yüksek çözünürlüklü fotoğrafın istenildiği zaman erişebileceği şekilde internette bulundurulması amaçlanıyorsa, FTP sunucuları bu amaç için en hızlı ve en iyi çözüm olacaktır. Fakat özel bir yazılıma ihtiyaç duymadan ve hiç bir ücret ödemeden de istenilen fotoğraf albümlerinin oluşturulabilmesi mümkündür. Bunun için sadece Yahoo veya Mynet gibi ücretsiz e-posta servislerinden birine kayıt olmak yeterlidir.

Her tür içeriğin yayınlanmasında özel web siteleri oluşturmak etkili yöntemlerden biridir. Bireysel web siteleri ile istenilen içerik kolayca ücretli veya ücretsiz olarak yayınlanabilir. Siteleri internette yayınlamak için iki ürün/hizmet kullanılır. Bunlardan biri, sitelere erişebilmemizi sağlayan “google.com”, “youtube.com” gibi site adreslerdir. Bu adreslere **domain** veya **alan adı** denir. Alan adını kullanarak siteye girmeye çalıştığımızda, site dosyalarının depolandığı sunucuya bağlanırız ve site sayfalarını ziyaret edebiliriz. Site dosyalarını barındıran sunuculara ise **web alanı, web hosting** veya **hosting paketi** denmektedir. Hazırlanan bir sitenin diğer internet kullanıcıları tarafından ziyaret edilebilmesi için öncelikle bir web hosting paketi alınarak buraya göndermesi ve siteye ulaşılabilmesi için bir alan adı alınarak sunucuya yönlendirilmesi gerekmektedir. Bu amaçla çalışan çok sayıda kuruluş bulunmaktadır.

1.4.3.3 Çevrimiçi Bağlantılarda Alınması Gereken Önlemler



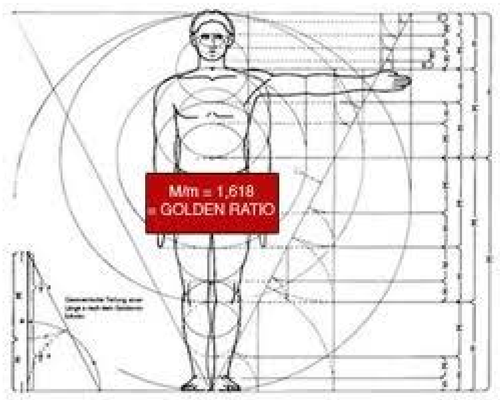
Çevrimiçi bağlantılarda özel bilgilerin paylaşılmasının riskli olduğu gerçeği hiçbir zaman unutulmalıdır. Özellikle sosyal ağlarda yaygın olarak kullanılan uygulamalara dikkat edilmesi, sitelerin güvenlik seviyelerine dikkat edilmesi, sosyal ağlar üzerinden alınan her mesaja itibar edilmemesi, kimlik hırsızlığına karşı kişisel bilgilerin gizli tutulması, arkadaş ekleme taleplerinde de seçici olunması gibi tedbirler sosyal ağlarda kullanıcıların dikkat etmesi gereken önemli başlıkları oluşturmaktadır. Ayrıca; Facebook, twitter, myspace, bloglar vb. sosyal ağlarda profillerin yabancılardan gizlenmesi gereklidir. Zira İnternetten edinilen kişisel bilgiler üzerine kurulan dolandırıcılık modelleri gün geçtikçe artmaktadır. Bu nedenle örneğin, Facebook hesabı açan herhangi birinin kişisel bilgilerinize ulaşmasını engellemek için profilinizin yalnızca arkadaşlarınızın görebileceği şekilde ayarlaması gereklidir. Ayrıca sosyal ağ sitesine giriş yaparken “Oturumumu sürekli açık tut” seçeneğinin işaretlenmemesi ve şifrelerin en az altı ayda bir güvenli bir şifre ile değiştirilmesi ve kapsamlı bir anti virüs internet güvenlik programı kullanılması, önemli bilgileri koruyan sosyal ağ şifrelerinin hiç kimseyle paylaşılmaması gereklidir.

Başkalarının her zaman sitenize erişebileceği unutulmamalıdır. Bilgi veya fotoğraflar tanınmayan kişilere gönderilmemelidir. Sosyal ağlarda paylaşılanı her türlü bilginin kötü niyetli kişiler tarafından kullanılarak kişisel bilgilerin elde edebileceği ve bu bilgilerin kötü amaçlı kullanabileceği bilinmelidir. Bu nedenle aşağıda sıralanan diğer önlemlere de dikkat edilmelidir. Gönderilen içeriğin ulaşılabilirliği sınırlandırılmalı, kimler ulaştığı bilinmelidir. Arkadaşlarınız ve takip ettikleriniz konusunda dikkatli olunmalıdır. Eklentilerden uzak durulmalıdır. Sosyal ağların sizin yerinize virüsleri taradığı düşünülmemelidir. Ağdaki linkleri tıklamadan önce dikkatle incelenmelidir. Her zaman web tarayıcının güncel versiyonu kullanılmalıdır. İşletim sistemi ve uygulamalar güncel tutulmalıdır. Sosyal ağlardan gelen e-postalara karşı ihtiyatlı olunmalıdır.

1.4.4 Sağlık

1.4.4.1 Ergonomi

Bilgisayarın günlük yaşantımızın bir parçası haline geldiği günümüzde milyonlarca insan bilgisayarları en başta gelen iş araçları olarak kullanmaktadır. İş dışına baktığımızda da son on yıl içerisinde insanların bilgisayar karşısında geçirdikleri sürelerin inanılmaz derecede arttığı görülmektedir. Bilgisayarların bu artan yoğun kullanımla birlikte birçok olumsuz etkinin ortaya çıktığı gözlemlenmektedir. Üstelik bilgisayarların olumsuz etkileri birçok etmenden dolayı çoğunlukla küçümsenmektedir. Oysa bilgisayarlar fiziksel, ruhsal ve zihinsel olarak kullanıcılarını etkilemenin yanı sıra maddi zararlar da verebilmektedir.



Ergonomiye kısaca "**fiziksel çevrenin insana uyumlaştırılması süreci**" diyebiliriz. Günümüz endüstri çağında makine-insan arasındaki artan ilişkiler, insana uyumlu çevre, eşya, makine, ofis vs. gibi fiziksel çevre birimlerinin yaratılması çabalarını zorunlu kılmaktadır. Öyle ki artık sadece fiziksel çevrenin ergonomisinden değil, doğrudan insanın zihnine seslenen bilgisayar yazılımları, Internet, web tasarımı vs. gibi öğelerin de insana uyumundan (Zihinsel algılama, kolay kontrol edebilme ve yönlendirebilme açısından) söz edilmektedir.

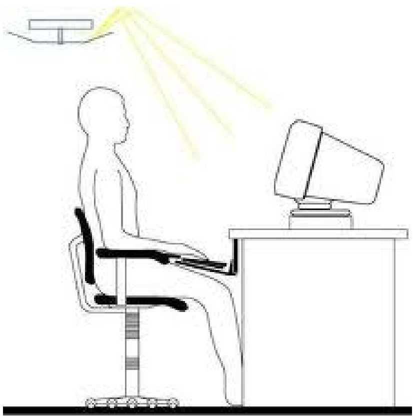
Bu anlamda ergonomi, birçok bilimsel disiplinin ortak çalışma alanı olan (Başta mühendislik, mimarlık, tıp, fizyoloji, anatomi, psikoloji, sosyoloji olmak üzere) bir yaklaşımlar bütünüdür. Tüm bu bilimsel disiplinler ortaklaşa bir insana uyumlaştırılmış ideal makine-çevre sisteminin arayışı içindedirler. Elbette ki bu arayışın temel amacı, sadece insanın kendisiyle barışık uyumlu bir çevrede yaşaması değil, en önemli üretim faktörü olan insan gücünün (ya da işgücünün) rahat, kolay ve sağlıklı bir şekilde üretim ve ekonomik faaliyetlerini sürdürebilmesini sağlayan makine, teçhizat, ofis, fabrika düzeni vs.nin yaratılması isteğidir. Çünkü bilinmektedir ki, insanın verimli çalışması, en iyiyi üretmesi ve ekonomik faaliyetlere en etkin şekilde katılabilmesi, bu ideal uyumun yakalanabilmesine bağlıdır.

Bilgisayar kullanırken daha iyi bir çalışma olması için uyulması gereken birçok etmen bulunmaktadır. Bunlardan bir kısmı ergonomik kökenlidir. Ergonomik kökenli olarak nitelendirebileceğimiz etmenler; çalışma alanı, masa, sandalye, ekran, fare, aydınlatma ve çalışma alışkanlıklarıdır.

1.4.4.2 Işığın Sağlık Açısından Önemi

Bilgisayar kullanımı için uygun olmayan ışık koşulları, göz yorgunluğu, göz yanması veya kaşınması, bulanık görme ve çift görme gibi görsel rahatsızlıkların en büyük nedenlerindendir. Birçok çalışma ortamındaki aydınlatma, en uygun ekran görüşü için çok parlaktır. Işık miktarı, aydınlatmayı sağlayan lamba veya flüoresan gruplarının seyreltilmesi (örneğin 4'lü bir flüoresan grubundan iki tanesinin çıkartılması) ile azaltılabilir. Odanın loş

ışıklı olması sağlanmalı, aydınlatma 30–50 mumluk ve endirekt olmalıdır. Ek bir masa aydınlatması okuma için tavan aydınlatmasından daha iyi bir seçenektir. Göz zorlanması ve göz yorgunluğunu azaltmak için uyulması gereken bazı kurallar bulunmaktadır. Örneğin; Parlamayı azaltmak için perde veya şerit perdeler kapatılmalıdır. Aydınlatma ekranda parlamayı engelleyecek şekilde ayarlanmalıdır (ışık kaynağı düşük watt'lı ve ekrana 90 derece açıda olmalıdır). Görüş alanı içerisinde yoğun ve düzensiz aydınlatmadan kaçınılmalıdır. Ekran mümkün olduğu ölçüde pencerelere 90 derece olacak şekilde yerleştirilmelidir. Mümkünse endirekt veya siperlenmiş aydınlatma kullanılmalıdır. Duvarlar yansıtıcı özelliği olan boya ile boyanmamalıdır. Tavan aydınlatmasının yarattığı parlamayı azaltmak için parlamayan ekran veya parlama önleyici monitör filtresi kullanılmalıdır (Bursa Sağlık Müdürlüğü, 2006).

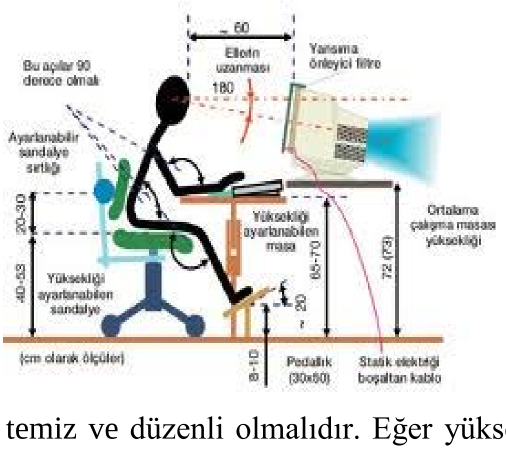


1.4.4.3 Bilgisayarı Doğru Pozisyonda Tutmanın Önemi

Çalışma Alanı: Çalışma alan, gerekli işleri gerçekleştirebilmek için tüm hareketlere olanak sağlayacak ve kullanıcısına uygun gelecek kadar gen olmalı ve çalışma ortamında bulunan donanımlara yeteri ka yer sunabilmelidir (Bursa Sağlık Müdürlüğü, 2006). Örneğ Uzun ve sık telefon görüşmeleri yapılıyorsa bir kulaklık-ahize sistemi kullanılmalıdır. En sık kullanılan eşyalar tam kullanıcının karşında bulunmalıdır. Bilgisayar çalışma sahasında aşırı eşya kalabalığından kaçınılmalı 2005).



Masa: Standart mobilyaların herkesin ihtiyacına cevap veremeyeceği unutulmamalıdır. Uzun boylu bir kişi için çalışma yüzeyinin yükseltilmesi gerekirken daha kısa boylu bir kişi masasının altında bir ayaklığa veya diğer aksesuarlara ihtiyaç duyabilir. Masa yüksekliği ortalama 65–70 cm. arasında olmalıdır. İnsanların aynı bilgisayarı ortak olarak kullandıkları durumlarda ayarlanabilir mobilyalar tercih edilmelidir. Masa üzeri, sık kullanılan nesneler kullanıcıya yakın duracak şekilde düzenlenmelidir. Böylece aşırı gerilime neden olacak uzanma hareketinden kaçınılmış olur (Keser, 2005). Çalışma yüzeyi parlama ve yansımaları azaltacak şekilde mat bir kaplamaya sahip olmalıdır. Masa altı alan, kullanıcının bacaklarına yer bırakacak ve bacaklarını esnetmesine olanak sağlayacak şekilde temiz ve düzenli olmalıdır. Eğer yüksekliği sabit bir masa kullanılıyorsa, buna dikey olarak yüksekliği ayarlanabilen bir klavye altlığı eklenmelidir. Telefon kullanılmayan elin tarafına konmalıdır (Sağ el kullanılıyorsa sol tarafa, sol el kullanıyorsanız sağ tarafa). Masa lambası, (eğer kullanılıyorsa) dokümanları aydınlatmak üzere ayarlarken, monitör üzerinde parlama yapmayacak veya doğrudan göze gelmeyecek bir şekilde yerleştirilmelidir. Klavye ile sürekli



birtakım dokümanlara bakılarak yazı yazılıyorsa, bir doküman tutucu kullanılması tercih edilmelidir (Bursa Sağlık Müdürlüğü, 2006).

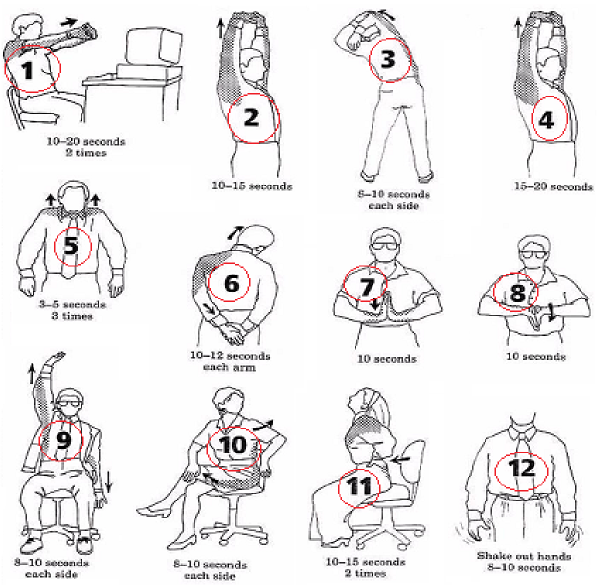
Sandalye: Oturma, sırta büyük ölçüde yük bindiren bir eylemdir. Uzun süre oturmak, intervertebral diskler (omurlar arasındaki süngerimsi yastıkçıklar) üzerinde artan basınçlara neden olmaktadır. Oturma, ayrıca bacaklar ve ayaklar üzerinde de olumsuz etkiler doğurur. Yerçekimine bağlı olarak kan bacaklarda ve ayaklarda toplanma eğilimi gösterir, bu da kanın kalbe dönüşünü yavaşlatır. Bu etkilerin giderilmesi için "Dinamik oturuş", tercih edilmeli, uzun süreler aynı sabit pozisyonda kalınmamalıdır (Bursa Sağlık Müdürlüğü, 2006).



Kullanılan koltuğun arkalığı bel için destek içermelidir. Koltuk arkalığınızın yüksekliğini sırt alt bölgesinin doğal içbükeyliğini destekleyecek şekilde ayarlanmalıdır. Sandalyenin yüksekliğini ayaklar yatay olarak zemine basacak şekilde ayarlanmalıdır. Sırt alt bölgesi arkalığa gelecek ve yine omuzların arkalığa temas edecek şekilde sandalyede dik oturulmalıdır. Bacaklar yere paralel olmalı ve dizler yaklaşık kalça ile aynı hizada olmalıdır. Dizlerin arka kısmı sandalyenin oturağı ile doğrudan temas etmemelidir. Oturağın ucu ile diz arkası arasında 5–10 cm mesafe bulunmalıdır. Kolçaklar çıkarılıp takılabilir olmalı ve iki kolçak arası mesafe ayarlanabilir olmalıdır. Kolçakların yüksekliği ve/veya genişliğini kullanıcının kollarını iki yanda dinlendirebileceği şekilde ayarlanmalıdır. Dirsekler ve kollar kolçaklar üzerinde hafifçe durmalıdır. Sandalye ve diğer donanım ayarlamaları ayakların yatay olarak yere temasını sağlamıyorsa bir ayaklık kullanılmalıdır. Bacaklarınızın üst kısmı ile masa altı arasında 5–10 cm mesafe kalmasına özen gösterilmelidir. Çalışma sürecinde arada bir kalkıp oturulmalı veya kısa yürüyüş molaları verilmelidir (Keser, 2005).

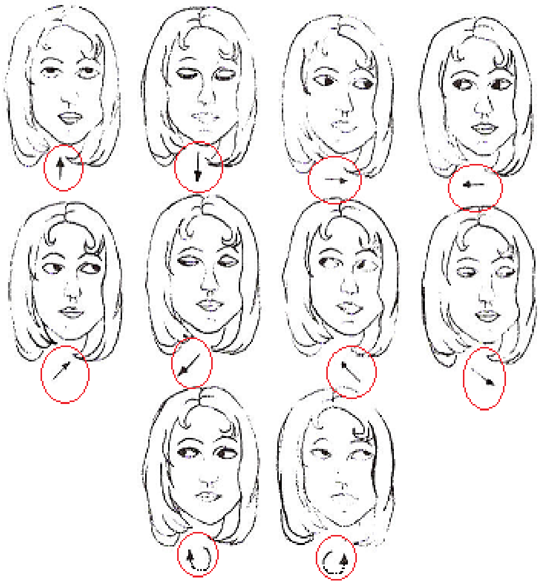
1.4.4.4 Bilgisayar Kullanırken Yapılacak Temel Hareketler ve Önemi

Tekrarlanan bilgisayarda çalışma statik çalışma şekli gözler için olduğu kadar, üst uzuvlar için de çok yorucudur. Bilgisayar başında çalışırken, vücudun dinlenmesi ve kendine gelebilmesi için 20–40 dakikada bir mola vermek bu nedenle önemlidir. Periyodik olarak pozisyon değiştirmek de önemlidir. Aynı pozisyonda sürekli oturmak veya kollara dayanarak uzun süre durmak dolaşımı bozabilmektedir.



Bilgisayar kullanımı sırasında verilen molalarda görme egzersizleri (15–20 dakikada bir kısa süre gözleri uzağa odaklayarak göz kaslarının dinlenmesi) yapılmalıdır. Saat başı daha uzun süreli mola verilerek çalışma ortamının temiz hava ile

doldurulması ve ufak beden egzersizleri (özellikle germe egzersizi) yapılması olumsuz etkilerin ortaya çıkmasını engelleyecektir (Keser, 2005).



Yukarıda ve yanda verilen temel esneme hareketleri ve göz rahatlatma teknikleri bilgisayar kullanımının bu açıdan yan etkilerini azaltmak için geliştirilmiştir.

1.4.5 Çevre

1.4.5.1 Geri Dönüşümün Önemi

Bilgisayar sarf malzemelerindeki artan maliyetler, uzmanları yazıcı kartuşlarının yenilenmesi ve geri dönüşümü konusunda araştırmalara yöneltmiştir. Bu çabaların sonucunda ekonomik anlamda tasarrufu ve çevreye verilen zararların azaltılması hedefleyen önemli bilimsel gelişmeler elde edilmiştir. Dolum kartuş kullanımı bu gelişmelerin bir sunucudur. Yazıcı kartuşları bittikten sonra atılmayıp doldurularak kullanılmaktadır. Siyah kartuşlar 3 ile 7 arası renkli kartuşlar 2 ile 4 arası tekrar dolum olanağı sunmaktadır. Dolum işlemi orijinal kartuştan hem ekonomiktir, hem de çevreye verilen zararı en aza indirgemektedir. Bu amaçla kartuş dolum makineleri kullanılmaktadır.

Orijinal yazıcı kartuşlarının tüketildikten sonra atılmayıp, yenilenmesi ve geri dönüşümü olgusu ekonomik anlamda son kullanıcı ve ülke çıkarları açısından giderek artan zorunlu bir eğilim haline gelmiştir. Bazı Avrupa ülkelerinde (İsviçre, Norveç, İsveç, Finlandiya, Danimarka, Avusturya, Hollanda, İspanya ve Çekoslovakya) uygulanan geri kazanım programlarında (European Recyling Program), kullanılmış kartuşlar toplanmakta ve kartuşta bulunan plastik ve metal malzemeler birbirinden ayrıştırılıp, bir üretim safhasından geçirilerek yeniden kullanılabilir hale getirilmektedir. Bu konudaki diğer bir örnek de bilgisayar sistemlerinde kullanılan pil, akü gibi enerji kaynaklarının ömürleri tamamlandıktan sonra atılmayıp geri dönüşüm merkezlerinde toplanmasıdır. Zira bunların doğaya bırakılması oldukça tehlikeli sonuçlar doğurmaktadır.



Elektronik metinlerin kullanılması basılı belge gereksinimini dolaysısıyla kullanılacak kâğıt miktarının azaltılmasını sağlayan en önemli faktördür. Eğer basılı belge kullanımı zorunluysa, artık ve kullanılmış kâğıtların ayrıştırılarak özel kâğıt toplama merkezlerine gönderilmesi gereklidir. Bu durumun çevre açısından oldukça önemli avantajlar sağladığı, toplanan atık kâğıtların tekrar kazanılmasıyla binlerce ağacın kesilmekten kurtarılacağı gerçeği unutulmamalıdır. Bu nedenle gerekmediği hallerde elektronik metinlerin kullanımı tercih edilmelidir. Doküman basımı ve çoğaltımı sırasında kullanılan toner, kartuş ve mürekkep gibi sarf malzemesi gerektirmediği gibi, gereksiz kâğıt tüketimini de engellemektedir. Bu özellikleriyle çevreye oldukça saygılıdır. Bu nedenlerle mümkün olduğu her durumda elektronik metinlerin kullanımı tercih edilmelidir.

1.4.5.2. Enerji Tasarrufu

Bilgisayarlar dünyada en hızlı elektrik yükü oluşturan cihazlardır. Gelecek yıllarda bu miktar giderek artacaktır. Ancak bilgisayarların kullandığı enerjinin çoğu, bilgisayar kullanılmadığı esnada açık olmasından dolayı boşa harcanmaktadır. Bunu engellemek için aşağıda verilen kurallara uyulmalıdır.



İş gününün sonunda bilgisayarlar ana monitörler düğmeden kapatılmalı veya uygun olduğu durumlarda, priz bağlantısı kesilmelidir. Böylelikle, bilgisayarların bekleme modunda harcadığı gereksiz enerji tüketimi önlenmiş olacaktır. İşletim sistemindeki güç yönetimi ayarlarını düzenlediğinizde, bilgisayarın güç kullanımını, iş ritmimize en azından kısmi olarak uyacak şekilde uyarlayabiliriz. Verimsiz çalışmadan kaçınarak enerjiden büyük miktarda tasarruf etmek gerçekten de mümkündür. Masaüstü veya dizüstü bilgisayarların güç yönetimi değerleri en düşük enerji tüketimi için önerilen ayarlar ayarlanmalıdır. Bu amaçla geliştirilen birçok uygulama bulunmaktadır. Örneğin Microsoft tarafından ücretsiz olarak sunulan Verdiem's Edison uygulaması işletim sisteminin mevcut güç ayarlarını daha fazla güç tasarrufu yapacak şekilde geliştirdiği ileri sürülmektedir.

Dizüstü bilgisayarlar, daha az enerji kullandıkları için daha az ısı üretir. Bu nedenle, bir masaüstü bilgisayar olarak dizüstü bilgisayar kullanmayı düşünmek enerji tasarrufu için daha iyi bir seçenektir. Yeni bir bilgisayar alınacaksa etiketi kontrol edilmelidir. Çevre Dostu ürünler tercih edilmeli ve bilgisayarın hangi standartlara uygun olduğuna bakılmalıdır. Avrupa Komisyonu'nun, ENERGY STAR eko-etiketi ve modern ofis bilgisayarlarındaki güç tüketimi ile ilgili olarak sunduğu ayrıntılı bilgileri www.eu-energystar.org adresinde bulunmaktadır. Bu web sitesinde bilgisayarlar, monitörler ve görüntüleme ekipmanı ile tüketiciler için bir güç hesaplama aracı sunulmaktadır. Güç hesaplama aracı, çok sayıda faktörü göz önünde bulundurarak, güç tüketimi ve genel masraflar ile ilgili ayrıntılı bir karşılaştırmalı hesap yapılmasını sağlamaktadır.

1.5 Güvenlik

1.5.1 Kimlik / Doğrulama

1.5.1.1 Kullanıcı Adı ve Şifre Kullanımı

Bilgisayar üzerindeki kişisel hakların ve verilerin korunması temelde bir kullanıcı hesabına dayanır. Bir bilgisayar sistemi farklı kişiler tarafından kullanıldığı durumlarda, kişisel hakların ve verilerin korunabilmesi için kullanıcılar arasında ayrım yapma gereği ortaya çıkmaktadır. Bir ağ sistemini kullanmak söz konusu ise bu kaçınılmaz bir gerekliliktir. Bu sayede kişiye özel dosyalar kişisel hale getirilebilmektedir. Bu yapılmadığı durumlarda kişisel haklardan ve verilerden bahsetmek pek mümkün değildir. Pek çok bilgisayarda olduğu gibi, tek bir kullanıcı varsa bile bunu yapmak faydalı olabilir. Sonuçta, her kullanıcı için benzersiz bir kullanıcı ismi verilmekte ve herkes bağlanmak için kendi bağlantı ismini ve şifresini

kullanmaktadır. Bununla birlikte kullanıcı için bir isimden ve şifreden daha fazlası mevcuttur. Bir kullanıcı hesabı, kullanıcının ismini, dosyalarını, kaynaklarını, erişim haklarını ve ona ait her şeyi temsil etmektedir.



Ağ güvenliği açısından kimlik sınaması; alıcının, göndericinin iddia ettiği kişi olduğundan emin olmasıdır. Bunun yanında, bir bilgisayar programını kullanırken bir parola girmek de kimlik sınaması çerçevesinde değerlendirilmelidir. Günümüzde kimlik sınaması, sadece bilgisayar ağları ve sistemleri için değil, fiziksel sistemler için de çok önemli bir hizmet haline gelmiştir. Bilgisayara giriş yaparken kullanıcı adı ve şifre kullanımında amaç kişinin önceden tanımlanmış kimliğe sahip kişi olduğunun tespit edilmesidir. Bu ispat bir şifre, bir akıllı kartın kullanımı, tek seferlik bir şifre, bir sayısal imza bilgisi, biyometrik bir özelliğin belirlenmesi şeklinde de olabilmektedir. Kullanıcı adı ve giriş şifresi, en yaygın kullanılan kimlik sınama biçimidir.

1.5.1.2 Şifre Koruma Politikaları



Kullanıcı adı ve giriş şifresi kullanım kolaylığı sunan bir uygulamadır. Fakat bu kolaylık başkalarının bu bilgileri eline geçmesini de kolaylaştırmakta olduğundan güvenlik boşluğu oluşturmaya adaydır. Bununla beraber şifreyle ilgili koruma politikaları ve uyulacak birkaç basit kural, şifrenin başkalarının eline geçmesini engelleyecektir: Öncelikle şifreler çok uzun süre kullanmamalı, belli aralıklarla değiştirilmelidir. Asla başkalarıyla paylaşılmamalıdır. Eğer bir kullanıcı kimliği yanlış şifreyle defalarca sisteme girmeye çabalıyorsa, bu şifrenin tahmin edilmesine yönelik bir çalışma olabileceği göz ardı edilmemelidir. Sistem, belli bir sayıda yanlış girişten sonra bu kullanıcının erişim hakkını askıya alarak, kendini ve asıl bu kimliğe sahip olan kullanıcıyı koruyacak şekilde düzenlenmelidir. Kesinlikle boş şifre kullanılmamalıdır. Şifre en az 8 karakter olmalı içinde, harf, rakam, diğer özel karakterler (%, !, ?, = gibi) grubundan en az birer karakter içermelidir. Şifre, bilinen ya da tahmin edilebilecek bir kelimeden (soyad, evcil hayvan adı, şehir adı gibi) ya da sözlüklerde bulunan sözcüklerden oluşmamalıdır (Pro-G, 2006).

1.5.2 Veri Güvenliği

1.5.2.1 Harici Veri Yedeklemenin Önemi

Veri güvenliği en genel anlamıyla, bir bilgisayar sistemini işlevsel kılan temel birimlerin, üzerinde çalışan yazılımların ve depolanan verilerin, arıza, hata, hasar durumlarında çalışmaların kesintiye uğramasını ve/veya verilerin geri dönülemez biçiminde kaybolmasını engellemek amacı sağlayan işlemler bütünüdür. Veri güvenliğinin birçok boyutu olmasına rağmen temel işlev; bir sistemin yedeğini almak ve bunu düzenli olarak yürütmektir. Bu zor bir süreç olmasına karşın bir gün herhangi bir nedenle bilgisayar sisteminin devre dışı kalması,

verilerin kaybolması ya da bozulması konunun önemini de ortaya çıkarır. Sürekli ve tutarlı bir şekilde, çalışılan verilerin yedeğini almak, bir gün yaşanacak bir saldırı ya da doğal bir afetin sonuçları bizi en az şekilde etkilemesini sağlayabilir. Bir yedek alma sisteminin kurulmasının maliyeti, üretilmesi uzun zaman alan verilerin kaybedildikten ya da veritabanındaki tüm kayıtlar silindikten sonra yeniden kazanma maliyetinden çok daha düşüktür.

Bilgisayar sistemlerindeki her verinin yedeği alınmamalıdır. Bu tür bir yedeklemede veriler, çevrim-içi ve çevrim-dışı şekilde aktarılabilir. Çevrim-içi aktarımda veriler, farklı bölgedeki merkeze, periyodik olarak bilgisayar ağı üzerinden aktarılır. Çevrim-dışı yolu ile yapılan yedeklemede ise, veriler, yüksek kapasiteli bir saklama ünitesi (teyp, flash bellek, taşınabilir hard disk, CD-RW, DVD-RW gibi) üzerine yazılarak güvenli bir şekilde saklanmalıdır.

Sistemlerin, elektrik kesilmelerine ve güç kaynağı arızalanmalarına karşı korunması da yedekleme konusunda ele alınabilir. Elektrik kesilmesi, hem kesinti boyunca çalışmanın durmasına neden olur, hem de çalışan sunucuda geri dönülemez donanım ya da yazılım arızaları meydana gelebilir. Bu tür durumlardan korunmak amacıyla, sistemler kesintisiz güç kaynakları ve yedek güç üniteleri ile desteklenmelidir.



Kişisel bilgisayarlar, doğaları itibariyle çok çeşitli amaçlar için kullanılabilirler. Bireysel örnekler vermek gerekirse İnternet erişimi, metin düzenleme, hesap tabloları ile mali durum izleme, fotoğraf işleme, müzik dinleme, e-posta kullanımı, oyun oynama, eğitim gibi amaçlar sayılabilir. Bu amaçlarla kullanılan bir bilgisayar sistemi, yedeklenmemişse aşağıda açıklanan çeşitli kayıplara maruz kalabilir. Bunun önlenmesi harici yedeklemenin önemini orya koyar.

Enerji Kaybı: Hem bilgisayarın işlerliğinin kesintiye uğramasına, hem de donanımının zarar görmesine (ve dolayısıyla disklerdeki verinin kaybına) neden olabilen bir sorun, elektrik kesintileri ve enerji sistemi arızalarıdır.

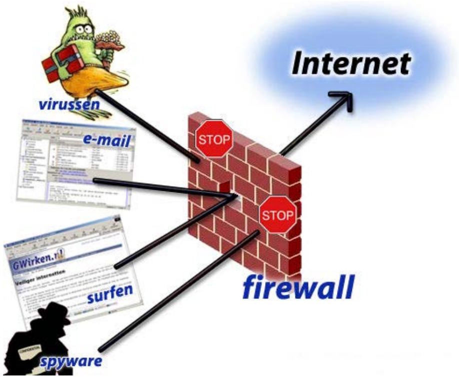
Donanım Kaybı: Depolama birimleri dışındaki donanımın hasar görmesi, veri kaybına yol açmayabilir, ancak işlerlik kesintiye uğrayacaktır.

Yazılım Kaybı: Burada yazılımdan kasıt, bilgisayarın işletimi için kullanılan ve kullanıcı tarafından üretilmiş verilerin dışında kalan tüm program ve program parçalarıdır. İşletim sisteminin kendisi, cihaz sürücüleri, uygulama programları, yardımcı programlar örnek olarak verilebilir.

Kullanıcı Ayarlarının Kaybı: İşletim sistemi ve programlar, kullanıcıların tercihlerine göre şekillendirilebilen pek çok özellik barındırırlar. Kullanıcı, kendi tercihleri doğrultusunda sistem ayarlarını yaparak bu ayarların kaydedilmesini sağlar. Bu ayarlar da doğal olarak sistemin depolama birimine kaydedilir. Depolama birimi hasar görürse veya yazılım işletiminde bir hata olursa, bu ayarlar kaybedilebilir.

Veri Kaybı: Herhangi bir uygulama programı ile oluşturulan herhangi bir dosya, yapılan herhangi bir kayıt, veri adı altında incelenebilir. Alınan ve atılan e-posta mesajları, yazılan metin dosyaları, yapılan çizimler, kaydedilen fotoğraflar hep bu başlık altında ele alınabilir.

1.5.2.2 Güvenlik Duvarı (Firewall)



Güvenlik duvarı, iki ağ arasındaki IP trafiğini kontrol etmek için kullanılan donanım veya yazılımlardır. Güvenlik duvarı, bir sistemin özel bölümlerini halka açık bölümlerden ayıran, kullanıcıların ancak kendilerine tanınan haklar düzeyinde sistemden yararlanmasını sağlayan çözümlerdir. Güvenlik duvarı belirli bir bilgisayarı denetlemek için o bilgisayar üzerine kurulabileceği gibi, bir bilgisayar ağını denetlemek için de kurulabilir. İçerideki/dışarıdaki sistemlere kimlerin girip giremeyeceğine, giren kişilerin hangi bilgisayarları ve hangi servisleri kullanabileceğini güvenlik duvarı üzerindeki kurallar belirler.

Güvenlik duvarı, bilgisayarları ve ağları dışarıdan gelebilecek tehditlere karşı filtrelemeye benzer bir yöntemle koruyan sistemlerdir. Bulundukları küçük bir veritabanı sayesinde birtakım kurallara sahip olurlar ve kurallara uymayan veri trafiğine izin vermezler. Örneğin bir güvenlik duvarı, belirli bir port üzerinden gelen bağlantı taleplerini reddedecek şekilde veya belirli bir IP numarasına bağlanılamayacak şekilde yapılandırılabilir. Güvenlik duvarı genel olarak; çeşitli ağ saldırılarına karşı bilgisayarı korumak, ağ trafiğini ve erişim politikalarını kontrol etmek ve herhangi bir şüpheli durum tespit edildiğinde uyarı göndererek durumu kullanıcıya bildirmek için kullanılır.

Güvenlik duvarının bir bilgisayarı tek başına kesinlikle koruyamayacağı unutulmamalıdır. Kesinlikle kullanılması şart olmasına rağmen güvenlik için tek başına yeterli değildir. Güvenlik duvarının en etkili şekilde çalışabilmesi, birçok parçadan oluşan bir güvenlik mimarisi içinde bulunmasına bağlıdır.

1.5.2.3 Veri Hırsızlığının Önlenmesi



Günümüzde veri hırsızlığının giderek yaygınlaşmaktadır. Kredi kartı bilgileri, kimlik numaraları, finansal kayıtlar ve ATM şifrelerini en çok çalınan verilerdir. Bu veriler 3 ana tip olarak sınıflandırılmaktadır: Kimlik hırsızlığı, kurumsal veri hırsızlığı ve çalıntı dizüstü bilgisayarlar veri hırsızlığıdır. Veri hırsızlığından korunmak için her şeyden önce internete bağlanmak için kullanılan hattın ve donanımın güvenli olup olmadığından emin olunmalı, güvenliği kuşkulu, halka açık noktalardan kişisel verileri kullanmayı gerektiren uygulamalar ve sitelere giriş yapılmamalıdır.

Kimlik hırsızlığı veri hırsızlığının özel bir şeklidir. Genellikle çalınan kişisel bilgiler; bu kişinin tam adı, konut veya resmi adresi, doğum tarihi, sosyal güvenlik numarası, e-posta adreslerini ve şifrelerini, telefon numaraları, aile üyelerinin bilgilerini, kredi kartı numaraları

ve banka hesap bilgilerinden oluşmaktadır. Hırsız kurbanın banka hesapları ya da diğer gizli bilgilere erişmek için çalınan kişisel bilgileri kullanma eğilimindedir. Çalınan kişisel bilgiler de taklit veya kâr için üçüncü taraflara satılan kullanılabilir. Veri hırsızlığından korunmak için aşağıda belirtilen önlemler alınmalıdır.

Fiziksel Güvenlik: Bilgisayar ve aksesuarları Kensington kilidi gibi fiziksel bir taşınmaz zincir ile bağlanarak güvenlik altına alınabilir.

Biometrik Güvenlik: Güvenlik şifreleri kullanılması zorunlu olmakla birlikte kırılmasının kolay olması nedeniyle biyometrik tanımlayıcıların kullanılması daha etkilidir. Zira biometrik şifrelerin aşılması neredeyse olanaksızdır. Bu biyometrik sistemler, kullanıcının bilgisayarı kullanmaya yetkisi olup olmadığını tespit etmekte yetkisiz bir kişinin bilgisayarı kullanmasını engellemektedir.

Gizlemek: Dramatik laptop hırsızlığı riskini azaltmak için düz bir taşıma kılıfı ya da sırt çantası kullanılmalıdır. Açıkta bırakılmamalıdır. Laptop hırsızlığı sonrasında önemli verilere erişim engellemek için aşağıdaki önlemler alınmalıdır.

BIOS Parola Koruması: BIOS parola koruması veri hırsızlığı olasılığında laptop sahipleri için önerilen bir seçenektir. BIOS şifresi girilmeden herhangi bir işletim sistemi çalışmayacaktır. Bu yöntem aşılamaz değildir; birçok üreticinin BIOS bypass şifreleri için arka kapı tuş kombinasyonları bulunmaktadır. Yine de, BIOS parola koruması çoğu veri hırsızlığını engelleyecektir.

Karmaşık Şifreler Kullanmak: Farklı sayı ve harf kombinasyonlardan ile büyük harfler ve sembollerden oluşan karmaşık şifrelerin kırılması zorlaşmaktadır.

Disk Şifrelemek: Sabit sürücüdeki tüm verileri şifreleme önemli bir veri koruma biçimidir. Tam disk şifreleme, bilgisayar üzerinde çalışan bütün verileri korur ve kullanıcıların sadece bir kez bilgisayara erişim için şifre girmesi gerektirecek kadar kullanımı kolaydır.

Sabit Disk Şifre Güvenlik Kilidi Kullanmak: Şifre güvenlik kilidi ile bir sabit disk içine ulaşmak neredeyse imkânsızdır. Kimsenin doğru şifreyi girmeden sürücü erişebilmesi mümkün değildir. Ayrıca, bu güvenlik kilidi sayesinde sabit disk başka bir bilgisayar üzerine takılsa da yeniden biçimlendirerek sıfırlaması da mümkün değildir.

Dosyalarınızı İçin Şifre Koruması Kullanmak: İşletim sistemleri ve birçok ücretsiz yazılım, önemli dosya ve klasörlerin koruması için güvenli kullanım şifresi sağlamaktadır. Bunu kullanmak bilgisayarınıza saldırı şansını azaltır.

1.5.3 Virüsler

1.5.3.1 Bilgisayar Virüsü



Bilgisayar virüsleri, bilgisayarın çalışmasını engelleyecek, verileri kaydedecek, bozacak veya silecek ya da kendilerini İnternet üzerinden diğer bilgisayarlara yayarak yavaşlamalara veya başka sorunlara neden olacak şekilde tasarlanmış yazılım programlarıdır. Bilgisayar programlarına istem dışı olarak eklenmekte ve programların yapması gereken asıl fonksiyonlarını hiç yaptırmamakta, kısıtlamakta veya yanlış işlemler yaptırmaktadır.

Bilgisayar virüsleri muzip virüslerden oldukça zarar verici olanlarına kadar yeni ve çeşitli biçimlerde görülür. Virüsler genelde bilgisayarlara bir şekilde zarar vermek amacıyla en son programlama dilleri ile yazılan küçük programcıklardır. Kimileri yapısı itibarıyla sadece bulaştığı bilgisayarlara zarar verir, kimileri de ağ yoluyla diğer bilgisayarlara da zarar verir. Bulaştığı bilgisayarın sistem kaynaklarını sömürerek yavaşlamasına, sistem dosyalarını kullanılmaz hale getirerek sistemin çökmesine, güvenlik açıkları yaratarak sistemin her türlü saldırıya açık hale gelmesine neden olurlar. Daha da önemlisi en son çıkan virüslerin yaptığı gibi dahili bir posta sunucu kurarak adres defterindeki ve ağdaki kullanıcılara virüslü posta göndererek hem bulaştığı bilgisayarın çökmesine hem de ağ performansının düşmesine sebep olurlar. Özellikle internet kullanımının yaygınlaşması ve bilgisayarlar arasında sürekli bir bağın olması (ağ) virüslerin yayılmasını da hızlandırmıştır. Her gün yeni bir takım virüsler ortaya çıkmakta ve hızla yayılmaktadır.

1.5.3.2 Virüsün Bilgisayara Girme Yolları



Virüslerden korunmak amacıyla bir takım anti-virüs yazılımları geliştirilmiştir. Bu yazılımları kolaylıkla temin etmek mümkündür. Ancak anti-virüs programlarına da virüslere karşı tamamen güvenmek oldukça büyük bir yanılgı olacaktır. Çünkü anti-virüs programları ancak o zamana kadar olan virüsler hakkında bilgi içereceklerdir. Yani sizin anti-virüs programını makinenize yüklediğinizden sadece kısa bir sonra yazılan ve makinenize girebilecek olan bir virüse karşı bu program hiç bir koruyucu rol oynamayacaktır. Bilgisayarınızı virüslerden korumanın ve bilgi ve zaman kaybını azaltmanın en iyi yolu, kullanacağınız anti- virüs programlarının yanı sıra öncelikle virüslerin hangi yollarla bilgisayarınıza girdiğini öğrenmek ve ona göre genel bazı korunma tedbirleri almak olacaktır. Genellikle virüsler bir bilgisayar aşağıda belirtilen yollardan girmektedirler:

- Temiz olduğundan emin olmadığımız disketlerden, taşınabilir disk ve belleklerden.
- Bir program yüklemek amacıyla kullandığımız CD ve DVD’lerden,

- Ağ komşularından bağlı olduğumuz virüslü bir bilgisayardan (ağ paylaşımı açık olduğu durumlarda),
- e-postalardan ve e-posta yoluyla almış olduğumuz dosyalardan,
- Çeşitli karşılıklı görüşme programları ve bunlar aracılığıyla alınan dosyalardan
- Sosyal ağlarda yaptığımız paylaşımlardan.
- Çoğu zaman güvenirliği bilinmeyen web sayfalarında dolaşmak bile bilgisayarımızın güvenliğini tehlikeye atacak zararlı program parçacıklarının yerleşmesine neden olabilmektedir.

Gerek virüsler gerekse bilgisayar saldırıları konusunda yapılması gereken birçok şey vardır. Öncelikle bilgisayar kullanıcılarının artık bu kavramları yeterince bilen bilinçli kullanıcılar olmaları gerekmektedir. Aşağıda bilgisayar güvenliği konusunda (virüs ve saldırılara karşı) yapılması gereken bazı temel noktalar belirtilmiştir. Tabii ki virüs veya saldırının şekline göre daha teknik önlemlerde mevcuttur.

- İyi bir anti-virüs programı yüklenmesi ve bunun düzenli bir şekilde güncellenmesi,
- Kullandığımız bilgisayarda gelişi güzel her taşınabilir belleğin kullanılmaması,
- İşimize yarayacağını kesin olarak bilmediğimiz, güvenilir olmayan kişilerden aldığımız CD ve DVD'leri kullanmamak ve bunlardaki programları yüklememek,
- Ağ komşularına hiç bir zaman tam paylaşım vermemek. Paylaşım verilmesi gerekiyorsa mutlaka parolaya bağlı paylaşım verilmelidir. İş bitince mutlaka paylaşımın kaldırılmalıdır.
- Paylaşım esnasında virüs ve trojen açısından güvenirliğine emin olmadığımız bilgisayarlardan veri transferi yapmamak.
- Tanımadığımız kişilerden gelen e-mailleri gerekirse hiç açmamak, tanıdıklarımızdan gelenlerden ise özellikle dosya eki varsa dikkatli davranmak. Özellikle sonu .exe olan dosyalara karşı temkinli davranmak.
- Sohbet ortamlarından ve sosyal ağlarda tanımadığımız veya tam olarak güvenmediğimiz kişilerden kesinlikle dosya transferi yapmamak,
- Bilgisayarımızda kullandığımız programlara ait şifreler varsa bunlarda kesinlikle kaydedilir şekilde bırakmamak. Örneğin Outlookexpres gibi programlarda şifreyi kalıcı yapılmamalıdır. Bu programlar ancak size şifre sorularak kullanılır olmalıdır ayrıca kısa zaman aralıklarıyla bu şifreler değiştirilmelidir.
- Güvenlik açısından oldukça önem taşıyan bilgisayarlar gerekli olmadıkça ağa ve internete bağlanılmamalıdır.

Hiçbir şey bilgisayarın yüzde yüz güvenli olduğunu garanti edemez. Ancak, bilgisayarın güncel tutulması, güncel bir virüsten koruma yazılımı kullanılması ve virüs güvenliği konusundaki uyarılara dikkat edilmesiyle bilgisayarın güvenliğinin artırılması ve virüs bulaşma olasılığının azaltılması sağlanabilir. Hiçbir güvenlik yöntemi garantili olmadığı için, bir virüsle veya başka sorunlarla karşılaşma olasılığına karşı, düzenli olarak kritik dosyaların yedeklenmesi oldukça önemlidir.

1.6. Kanun

1.6.1 Telif Hakkı

1.6.1.1 Telif Hakkı Nedir?

Bir bilgisayar yazılımının, hak sahibinin izni olmadan ve telif hakkını ödemeden kopyalanması, lisanssız olarak kullanılması ya da izin verilenden fazla sayıda çoğaltılması gibi eylemler, **yazılım telif hakkı ihlali** olarak adlandırılmaktadır (Kuzu, Bilgisayar Nedir ?, 2006).

Bilgisayar programlarının, algoritmaların, matematiksel formüllerin patentli olarak korunması ve hakkın ihlali olmayan durumlarda fikri mülkiyet eserlerinin paralel ithalatına izin verilmesine yönelik olarak uluslararası düzeyde bir eğilim ortaya çıkmaktadır. Bu eğilim sonucunda, bilgisayar ortamında üretilmiş ürünlerin kullanılması durumunda telif hakkının korunması temel sorun olarak ortaya çıkmaktadır. Bu sorunların çözümü için çeşitli yol ve yöntemler geliştirilmektedir (Beliner, 2005).



Günümüzde, her türlü dağıtım ağı üzerinden transfer edilen dijital bilgiye bağlı hakların korunmasını amaçlayan teknik çözümler ortaya çıkmaya başlamıştır. Koruma altına alınan bilgileri, bu bilgilerin kullanım haklarını ve koşullarını, kullanım haklarının elektronik ödeme araçlarını tanımlamak için, Bilişim Teknolojisini Araştırma ve Geliştirme Avrupa Strateji Programı (ESPRIT) ve Elektronik Telif Hakları Yönetim Sistemi (ECMS) gibi projeler geliştirilmektedir. Bu tür sistemler aynı zamanda Otomatik Lisanslama Sistemini de içermektedir. Mevcut donanımların ve araçların, işlemlerin güvenliğini sağlayacak ve bilginin izinsiz kullanımını önleyecek standarda tabii koruyucu mekanizmalarla donatılması konusunda çalışmalar yapılmaktadır (Uzunay & Koçak, Bilişim Suçları Kapsamında Dijital Deliller, 2006).

1.6.1.2 Lisanslı Yazılım Nasıl Anlaşılır?



Yazılımın kompakt disk veya diğer bir taşınabilir ortamlarda dağıtılan materyaller üzerinde alınması durumunda üzerinde bir etiket bulunması gereklidir. Bu **Proof of License** (Lisans Kanıtı) etiketidir. Bu etiket, gerçek bir yazılım kopyası üzerinde bulunur ve yazılımın lisanslı kopya olduğunu gösterir. Geçerli olması için etiketin yazılım paketi üzerinde yada taşınabilir aygıtların arka kısmında yapıştırılmış olarak (genellikle işletim sistemi lisansı) bulunması gereklidir. Etiketin ayrıca alınması lisans kanıtı sayılmaz ve geçersizdir. Yazılımın lisanslı kullanıcısı olunduğunu kanıtlamak için üzerinde etiket olan paketin saklanması gereklidir (Beliner, 2005).

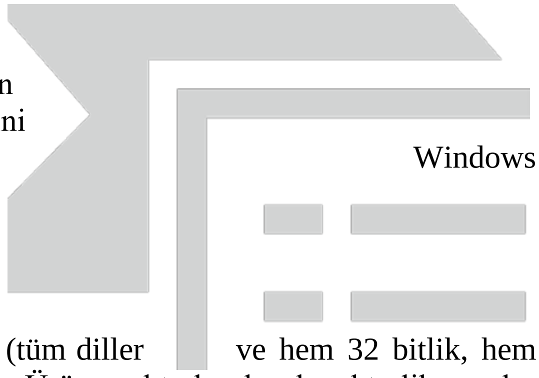
Yazılım Lisansı: Bir yazılım lisansı bir şahıs veya firmaya tanımlanmış bir şekilde yazılımı kullanma hakkı vermektedir. Lisans anlaşmasında ki şartlar yazılımın kullanımında ki kısıtlamaları açıklamaktadır. Ayrıca telif hakları yasası bir şahsın yazılımı nasıl kullanacağını şartlara bağlamaktadır. Örneğin bir kişi (veya firma) kullanılan her Microsoft yazılım programı için lisans anlaşması yapmak durumundadır.

Yapılan lisans anlaşmasına göre yazılım yükleme ve kullanmada çeşitli seçenekler ortaya çıkar. Örneğin çoğu lisans, yazılımın bir kopyasını tek bir bilgisayara, örneğin iş istasyonu, terminal veya sair bir aygıta (İş İstasyonu, Masaüstü Bilgisayar) yükleyebilme ve

buradayken kullanabilme, erişim sağlayabilme, görüntüleyebilme ve çalıştırabilme imkânı sunar. Yazılımın aynı anda tek bir iş istasyonu veya bilgisayarında ikiden (2) fazla işlemci tarafından kullanılmasına izin vermez.

A.B.D Telif Hakları Sözleşmesi ve uluslararası telif hakları anlaşmalarına göre telif sahibinden belirli kullanım hakkı alınmadan bilgisayar programlarının da içinde bulunduğu telif hakları alınmış materyallerin kopyalanması, kullanımı ve dağıtımı yasaklanmıştır. Satış, bedava dağıtım veya kişisel kullanım amacıyla yapıldığına bakılmaksızın, Bilgisayar yazılımlarının ve yazılım bileşenlerinin kullanım hakkı alınmadan yapılan çoğaltma, kullanımı veya dağıtımı telif hakları ihlalidir. Bilgisayar yazılımları, Fikir ve Sanat Eserleri Kanunu kapsamında yasal koruma altındadır. Bu nedenle lisanslamaya dikkat etmeli, lisansız yazılım kullanmamalıyız. Seri numaralarını kontrol etmeli, aldığımız ürünü kayıt ettirmeli, aldığımız yazılım ürününün lisansını görmeliyiz.

Ürün Kimliği Sınanması (PID): PID bir yazılım sisteminin her bir kopyasına özgü olan benzersiz bir kimlik numarasıdır. Yazılımın yüklenmesi sırasında, ürün tanımlayıcı bilgisini girmesini ister. Örneğin kullandığınız Microsoft Windows sürümünüzün geçerli bir lisansı olduğunu doğrulamak için ürün kimlik numarası ve ürün anahtarı kullanımını gerektirir.



Örneğin Windows 7 ailesinin tüm sürümleri (tüm diller ve hem 32 bitlik, hem de 64 bitlik sürümler) için ürün anahtarları gereklidir. Ürün anahtarları beş karakterlik gruplar halinde biçimlendirilmiş, çizgilerle ayrılmış 25 karakterlik alfa sayısal dizelerdir. Yazılımın kuruluşu sırasında yüklemeyi tamamlamak için ürün anahtarının girilmesi gerekir. Ürün anahtarının güvenli bir yerde saklanması ve başkalarıyla paylaşılmaması gerekir. Bu ürün anahtarı, o yazılımın yüklemesi ve kullanılabilmesi için temel oluşturur. Ürün anahtarı ayrıca, ürün kimliğinin de temelini oluşturur. Tüm lisanslı yazılımların birer benzersiz ürün kimliği bulunur. Ürün kimliğinde XXXX-XXXX-XXXX-XXXX gibi düzenlenmiş 5 ile 20 arasında alfa sayısal karakter bulunur.

Birçok yazılım ürününde, ürün etkinleştirme zorunludur. Ürün etkinleştirmenin amacı, yasadışı kopyalama veya "yazılım hırsızlığı" olarak da bilinen korsanlık biçimini en aza indirmektir.

1.6.1.3 Son Kullanıcı Anlaşması (EULA)

EULA (End User License Agreement - Son Kullanıcı Lisans Anlaşması) kullanıcının haklarını koruyan bir sözleşme olarak görünebilir. Aslında temel olarak EULA, kullanacağınız yazılımla ilgili gerekli yasal zorunlulukların hatırlatıldığı bir metindir. EULA genellikle yazılımı kurmadan önce önünüze getirilir ve kabul ettiğinizi belirtmek için metnin altındaki küçük bir kutuyu işaretlemeniz istenir. Yasalar karşısında bu, bir kâğıdın altına imza atmanızla eşdeğerdir. Çünkü o "kabul ediyorum" yazan küçük kutucuğu işaretlemeden yazılımın kurulmasına izin verilmez. Ancak genel olarak EULA, bürokratik bir zorunlulukmuş gibi görünse de, temelde yazılım şirketinin haklarını koruyan maddeler içerir.

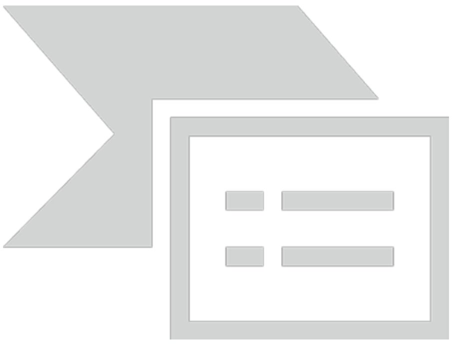
Yani Son Kullanıcı Lisans Anlaşması yazılım programının kullanımı hakkındaki lisansın hükümlerini belirlemektedir. Herhangi bir yazılım sistem üreticisi, yazılımına istinaden, PC Üreticisi ve son kullanıcı arasında yapılan lisans anlaşmasını kapsamaktadır. Lisans anlaşması yazılım ürününü üreten kurum ve son kullanıcı arasında gerçekleştirilir. Temelde yasadışı kopyalama ve paylaşım konusunda kullanıcı yükümlülüklerini içerir.



Yasadışı kopyalama, yazılımın son kullanıcı lisans sözleşmesi veya EULA'ya uymayan biçimde paylaşımı ve yüklenmesidir. Bu EULA kapsamında verilen lisans haklarıyla ortaya konmuştur. Lisanslı kopyaların yazılımın kurulum işlemleri sırasında açıklandığı şekilde etkinleştirilmesini gerektirir. Etkinleştirme için gereken bilgilerin verilmemesi halinde, yazılımın ilk defa yüklediği tarihten sonraki ilk otuz (30) gün içinde yapılması ile sınırlandır. Yazılımın İnternet veya telefon aracılığıyla da etkinleştirilebilmesi mümkündür.

EULA metinlerini okumanın kullanıcıya sağladığı en büyük avantaj, yazılımın kullanılması sırasında oluşan pek çok soruya cevap veriyor oluşudur. Örneğin pek çok kullanıcı bir yazılım satın aldığında aslında yazılım satın almadığını, sadece o yazılımı kullanma lisansı aldığını bilmez. Oysa yazılımın mülkiyeti ve onun üzerinden gerçekleşecek her türlü alışverişin, yazılımın kodlarının hakları hala yazılımı geliştiren veya dağıtan firmaya aittir ve kullanıcı belirli veya belirsiz bir süre için yazılımı kullanamaya izin almıştır.

1.6.1.4 Ücretsiz Yazılım ve Türleri



Public Domain Yazılımlar: Bu programları yazan kişiler, kendi programlarını herkesin alıp bedava kullanmasına izin verirler. Ancak, bazı durumlarda bu bedava kullanım kısıtlandırılır. Public Domain yazılımlar tamamı değiştirilmeden üçüncü kişilere kopyalanmalı, eğer söz konusu eser bir başka yerde kullanılacaksa (örneğin bir başka eserde bundan yararlanılacaksa) yazarlarına bildirilmeli, herhangi bir şekilde eserin dağıtımından dağıtım medyası masrafından fazla masraf alınmamalıdır. Bunun en iyi örneklerinden biri GPL (GNU Public License)'dir

Serbest (Freeware) Yazılımlar: Serbest yazılımlar limitsiz bir şekilde bunları alan kişiler tarafından kullanılabilir. Bu yazılımlar, parayla üçüncü kişilere satılmamalıdır. Lisans zorunluluğu bulunmamaktadır.

Paylaşımlı (Shareware) Yazılımlar: Shareware yazılımlarda ise **kullan, eğer beğenirsen bana belli bir miktar para gönder** felsefesi geçerlidir. Bu miktar genellikle 1–20 ABD doları aralığındadır. Paylaşımlı yazılımlar kaynak kodları ile birlikte dağıtılmayabilirler. Programı alan kişi, belirli bir süre (1 ay gibi) kullanır, eğer kullanmaya devam ederse bu parayı

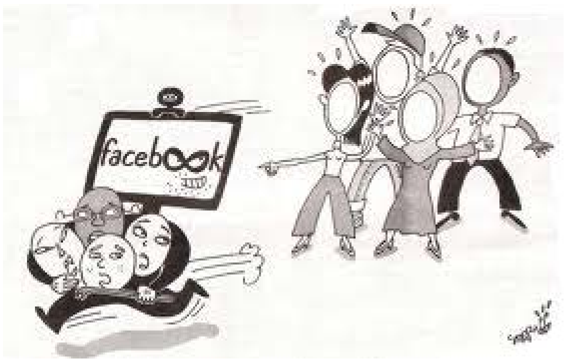
gönderir. Ancak, burada zorlayıcı bir mekanizma yoktur. Yine programı kullanırsınız ama para ödemezsiniz. Bazı durumlarda, kullandığımız paylaşımlı program, süresi dolunca çalışmaz.

Açık Kaynak (open-source) Yazılımlar: Açık kaynaklı yazılım, kaynağı açık yazılım veya açık kaynak kod aynı anlamda kullanılan terimlerdir ve kaynak kodu isteyen herkese açık olan yazılımlardır. Bu tür yazılımların ayırt edici özelliği kullanıcıya yazılımı değiştirme özgürlüğü sağlamasıdır. Açık kaynak kodlu yazılımlar, uyarlanabilir, sağlam, hızlı ve güvenlidir. Açık kaynak kod dünyası, yeni bir yazılım üretme biçimi, yeni iş modelleri sunmaktadır. Dünyanın her tarafından bilişim uzmanlarınca imece yöntemi ile endüstri standartlarında geliştirilen açık kaynak kod yazılımları, insanlığın ortak malıdır. Açık kaynaklı yazılımlar 2005 yılı itibariyle bir patlama yapmışlar ve on binlere varan yazılım ve varyanta ulaşmışlardır. En iyi bilinenler Linux, Open Office, GNU, Debian'dır.

1.6.2 Veri Koruma

1.6.2.1 Veri Koruma Nedir?

Bilişim güvenliğinde en önemli konularda biri, kaynaklara kimin nasıl eriştiğini kontrol etmek, bu sayede bilgi üzerinde yetkisiz değiştirme ve açığa çıkarma olaylarını engelleyerek verileri korumaktır. Bu amaçla yapılan faaliyetlere genel olarak erişim denetimi adı verilmektedir. Bir kullanıcı bilgisayarından ağ üzerindeki bir dizine ulaşmak istediğinde ona kullanıcı adı ve şifre soran bir ekranla karşılaşması, erişim denetimine örnek olarak verilebilir. Erişim denetimi, yazılım ve donanım tabanlı olarak sağlanabilir. Erişim denetimi yardımı ile kullanıcı ve sistemlerin, diğer sistemlerle nasıl etkileşimde bulundukları belirlenir. Erişim denetimi kontrolleri ile kaynaklara yetkisiz erişimler engellenir ve yetkili kullanıcıların da yetki derecelerine göre erişimleri sınırlandırılır. Erişim denetimi 1. Tanımlama, 2. Kimlik Sınama ve 3. Yetkilendirme olmak üzere 3 aşamada gerçekleştirilir (Çağlayan, 3-4 Ekim, 2003).



Tanımlama: Değerli bir kaynağa, yalnızca ona erişmeye hakkı olanlara erişim yetkisi verilmelidir. Bu erişim yetkisinin denetimi sırasında, kullanıcılardan iki tür bilgi istenir. Birinci bilgi herkesin bildiği kullanıcıya ait ve kullanıcının kimliğini belirten bir bilgidir. Sosyal güvenlik numarası, çalıştığı kurumdaki sicil numarası, kullanıcının adı soyadı, sistemden tanımlanmış kullanıcı adı, kullanıcı kimliğine örnek olarak verilebilir. İkinci tür bilgi ise, yalnızca kullanıcının bildiği özel bir bilgidir (Pro-G, 2006).

Kimlik Sınama: Bir kişinin önceden tanımlanmış kimliğe sahip kişi olduğunun tespit edilmesidir. Bu ispat bir şifre, bir akıllı kartın kullanımı, tek seferlik bir şifre, bir sayısal imza bilgisi, biyometrik bir özelliğin belirlenmesi şeklinde karşımıza çıkmaktadır. Giriş şifresi, en yaygın kullanılan kimlik sınama biçimidir. Kullanım kolaylığının yanında, başkalarının eline geçmesi kolay olduğundan dikkatli kullanılmalıdır.

Yetkilendirme: Sisteme kendini kimliği ile tanıtmış ve kimlik sınaması yapılmış (yani belirttiği kimliğe sahip olan kişi olduğunu ispatlamış) kullanıcılara, sistem kaynaklarına erişim izni verilmesidir. Kullanıcı, kimlik sınaması yapıldıktan sonra, ağ üzerindeki bir kaynaktaki bir dosyaya erişmek istediğinde, öncelikle bu kullanıcının bu kaynağa erişim yetkisi olup olmadığı sınanır. Eğer yetkisi varsa, kaynağa erişmesine izin verilir. Yani bir kullanıcı, kimlik sınaması yapıldıktan sonra, tüm kaynaklara erişme yetkisine sahip olmaz. Erişim yetkisi/hakkı, kendisine verilen yetki düzeyi ile sınırlıdır (Pro-G, 2006).

Veri güvenliği için verilerin sorumlu olduğu kişilere sorumluluk verilmesi, verilerin doğruluğunu sağlanması için gerekli önlemlerin alınması temel zorunluluktur.

1.6.2.2 Ülkemizde Veri Koruma

Gelişmiş ve gelişmekte olan ülkelerde olduğu gibi ülkemizde de veri koruma yasa ve anlaşmalarıyla bilişim güvenliği sağlanmaktadır. Bu amaçla geliştirilen yasa ve anlaşmalarla bilişim ürünleri güvence altına alınmaktadır.



Yeni Türk Ceza Kanununda telif haklarıyla ilgili düzenlemelere yer verilmiştir. Ayrıca Telif Hakları Kanunu, Telif Hakları ve Sinema Genel Müdürlüğü, 5.12.1951 Tarihi ve 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nda Bilgisayar programı, Arayüz, Araişlerlik ve telif hakları ile ilgili diğer düzenlemeler yer almaktadır (Eker, 2006).

Tüm bu kanunlara göre bilgisayar programları yazılım hakkı sahibinin izni olmaksızın kopyalanamaz, bedelli ve bedelsiz dağıtılamaz, kiralanamaz, izinsiz bir başka ülkeden ithal edilemez. Yazılım korsanlığı yapan her kişi ve kuruluş aslında hırsızlık yapmış sayılır ve Fikir ve Sanat Eserleri Kanunu (FSEK) gereğince cezalandırılır.

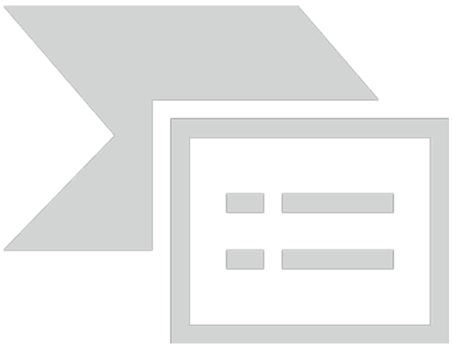
3 Mart 2001'de Fikir ve Sanat Eserleri Kanunu'nda yapılan değişikliklerle korsan yazılım kullanılması, kopyalanması veya satışı halinde uygulanacak cezalar şöyle şekillenmiştir: Eksik her bir lisans başına 24-121 milyar TL para cezası; 2 seneden 6 seneye kadar, paraya çevrilmeksizin hapis; 3 seneye kadar meslekten men; korsan yazılım yüklü bilgisayarlara el konulması. Görüldüğü gibi korsan yazılım kullanımının cezası oldukça ağırdır (Dülger, 2006).

15.1.2004 tarihli ve 5070 sayılı Elektronik İmza Kanunu (R.G: 23.1.2004 – 25355). Bu kanunla; ekonomik ve teknolojik gelişmeye bağlı olarak elektronik ticaretin uygulamaya sokulması sonucu kullanıma açılan elektronik imzanın hukuki ve kurumsal anlamda yapısı düzenlenmiştir.

Kişisel Verilerin Korunması Kanunu Tasarısı (Sevk Tarihi: 09.11.2005). Bu tasarıyla; kişisel nitelikteki verilerin tanımının yapılması, esas ve unsurlarının belirlenmesi ve korunması amacıyla idari bir yapının oluşturulması ile bireylerin şahsiyet haklarının himayesine ilişkin düzenlemeler getirilmesi amaçlanmaktadır.

İnternet yoluyla işlenen suçlar hakkında kanun tasarısı komisyonu çalışmaları. Avrupa Konseyinin 186 sayılı Siber Suçlarla Mücadele Sözleşmesi ile yabancı ülke mevzuatlarından da yararlanılarak, ülkemizde giderek yaygınlaşan İnternet kullanımı sonucu ortaya çıkan suçların cezalandırılabilmesi ve Türk Ceza Kanununda bu konuda mevcut boşluğun doldurulması yönünde hükümler içeren yeni bir kanun tasarısı hazırlanmış ve İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik 30.11.2007 tarihinde resmi gazete de yayınlanmıştır.

1.6.2.3 Ülkemizde Veri Koruma Sorumluluğu



1997 yılında Emniyet Genel Müdürlüğü İstihbarat Daire Başkanlığı bünyesinde İletişim ve Veri Güvenliği Bürosu kurulmuştur. Daha sonra İnternet Suçları ile Mücadele Amirliği faaliyetlerine başlamıştır. 1999 yılında Bilgi İşlem Daire Başkanlığı bünyesinde Bilişim Suçları Çalışma Grubu oluşturulmuş ve halen Bilişim Suçları Araştırma Büro Amirliği olarak görevine devam etmektedir. 2000 yılında TADOC (Türkiye Uluslar Arası Uyuşturucu ve Organize Suçlarla Mücadele Akademisi) kurulmuş, yine aynı akademi bünyesinde Bilişim Suçları Araştırma Merkezi faaliyete geçirilmiştir.

Ulaştırma Bakanlığı bünyesinde, internet kullanımının Türkiye'de sağlıklı gelişmesi ve toplumsal yarar sağlanması ve temel öneriler oluşturulması için İnternet Kurulu kurulmuştur. Kamu kurum ve kuruluşları da kendi ilgi alanlarına giren konularda internet güvenliği ile ilgili çalışmalar yapmaktadırlar.

Bilişim suçlarıyla mücadele konusunda eğitim verilmesi ve personel yetiştirilmesi konusunda çeşitli üniversitelerce kurulmuş enstitü, kurul ve çalışma grupları teşkil edilmiştir. Bu alanda toplumu bilgilendirme ve eğitim konularında faaliyet gösteren sivil toplum kuruluşları da bulunmaktadır.

Jandarma Genel Komutanlığında 2001 yılında İnternet İstihbarat Kısmı ve 2003 yılında "Bilişim Suçları Kısmı" kurulmuştur. Bu birimler İl Jandarma Komutanlıkları ile koordineli olarak çalışmaktadır.